

目录

前言	1.1
Mach-O概览	1.2
背景知识	1.2.1
XNU	1.2.1.1
编译链接加载过程	1.2.1.2
PIC	1.2.1.3
Mach-O格式	1.3
Mach-O结构概述	1.3.1
Mach-O结构图	1.3.1.1
Mach-O结构详情	1.3.2
Header	1.3.2.1
magic	1.3.2.1.1
cputype和cpusubtype	1.3.2.1.2
filetype	1.3.2.1.3
flags	1.3.2.1.4
Load Commands	1.3.2.2
LC_UUID	1.3.2.2.1
LC_SEGMENT	1.3.2.2.2
LC_SEGMENT_64	1.3.2.2.3
LC_SYMTAB	1.3.2.2.4
LC_DYLD_CHAINED_FIXUPS	1.3.2.2.5
LC_DYLD_EXPORTS_TRIE	1.3.2.2.6
Segment	1.3.2.3
__TEXT	1.3.2.3.1
__text	1.3.2.3.1.1
__DATA	1.3.2.3.2
__la_symbol_ptr	1.3.2.3.2.1
__got	1.3.2.3.2.2
__IMPORT	1.3.2.3.3
__LINKEDIT	1.3.2.3.4
__OBJC	1.3.2.3.5
Section	1.3.2.4
symbol	1.3.2.4.1
string	1.3.2.4.2

FAT	1.3.3
举例	1.3.3.1
常见问题	1.3.3.2
工具	1.3.3.3
lipo	1.3.3.3.1
codesign	1.3.4
虚拟地址	1.3.5
大小限制	1.3.6
Mach-O工具	1.4
MachOView	1.4.1
举例	1.4.1.1
main_arm64	1.4.1.1.1
AwemeCore	1.4.1.1.2
zzzzHeiBaoLib.dylib	1.4.1.1.3
心得	1.4.1.2
自己编译	1.4.1.2.1
rabin2	1.4.2
用法	1.4.2.1
举例	1.4.2.2
AwemeCore	1.4.2.2.1
MaskPro.dylib	1.4.2.2.2
help	1.4.2.3
jtool2	1.4.3
用法	1.4.3.1
举例	1.4.3.2
AwemeCore	1.4.3.2.1
MaskPro.dylib	1.4.3.2.2
akd	1.4.3.2.3
help	1.4.3.3
otool	1.4.4
用法	1.4.4.1
举例	1.4.4.2
Aweme	1.4.4.2.1
AwemeCore	1.4.4.2.2
MaskPro.dylib	1.4.4.2.3
help	1.4.4.3
pagestuff	1.4.5

help	1.4.5.1
附录	1.5
Mach-O文档和资料	1.5.1
参考资料	1.5.2

可执行文件格式：Mach-O

- 最新版本: v1.0.0
- 更新时间: 20231007

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、编译链接加载过程、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的数据；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

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

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

鸣谢

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

其他

作者的其他电子书

本人 crifan 还写了其他 150+ 本电子书教程，感兴趣可移步至：

[crifan/crifan_ebook_readme: Crifan的电子书的使用说明](#)

关于作者

关于作者更多介绍，详见：

[关于CrifanLi李茂 – 在路上](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 23:27:54

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

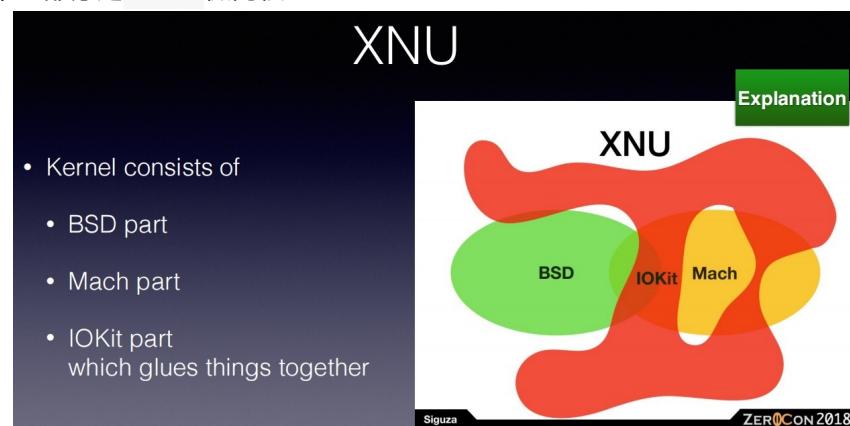


WHERE IS IT FOUND?

- /Applications/
- /Library/
- /usr/bin/
- /Cores/
- /System/



- 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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-04 17:52:09

XNU

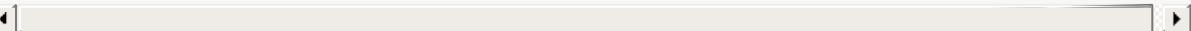
- XUN
 - 名称
 - XNU = **X** is **N**ot **U**nix
 - 概述
 - 英文
 - XNU kernel is part of the Darwin operating system for use in macOS and iOS operating systems.
 - 中文
 - XNU是：iOS（和tvOS、watchOS）的（操作系统）内核
 - XNU也是Darwin的一部分
 - Darwin是MacOS的操作系统内核
 - 特点
 - XNU is a hybrid kernel combining the Mach kernel developed 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 \(apple.com\)](https://sourceBrowser.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
```



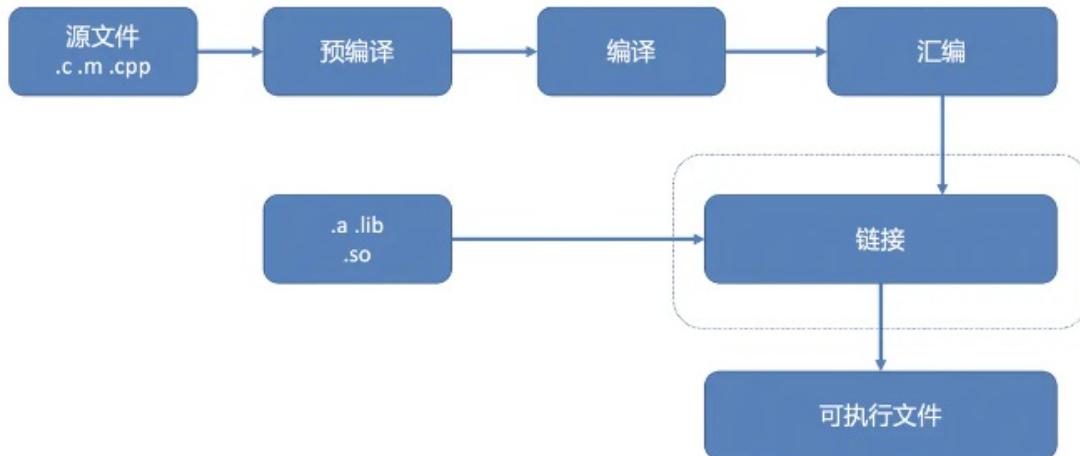
- xnu-8019.12.5~1/RELEASE_ARM64_T8015

- xnu是：iOS的内核
- 版本是：8019.12.5

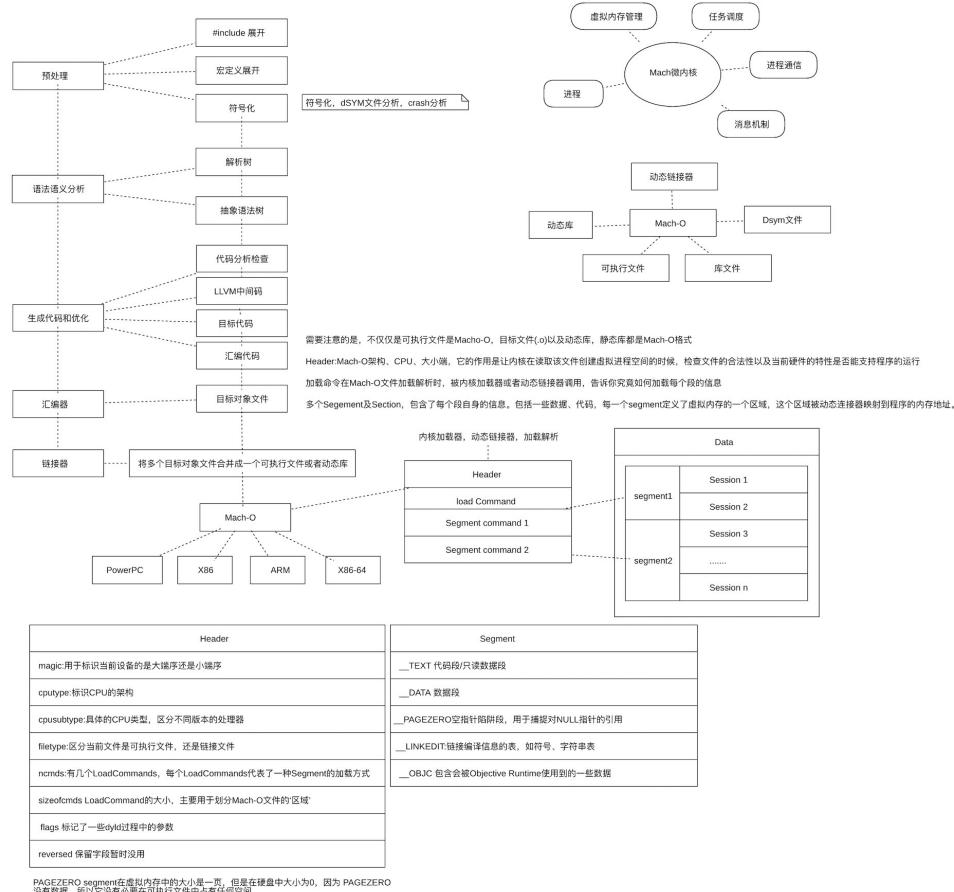
编译链接加载过程

- 编译链接加载过程

 - 概述



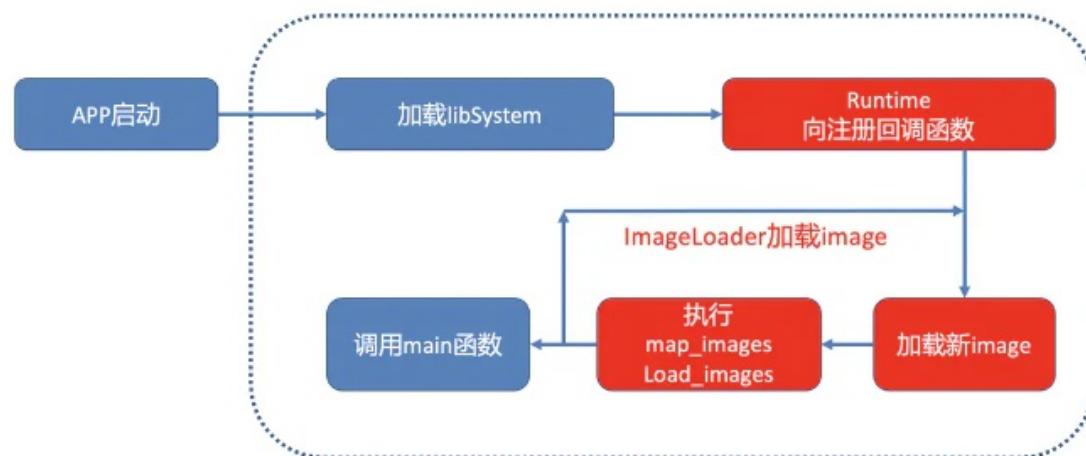
 - 详解



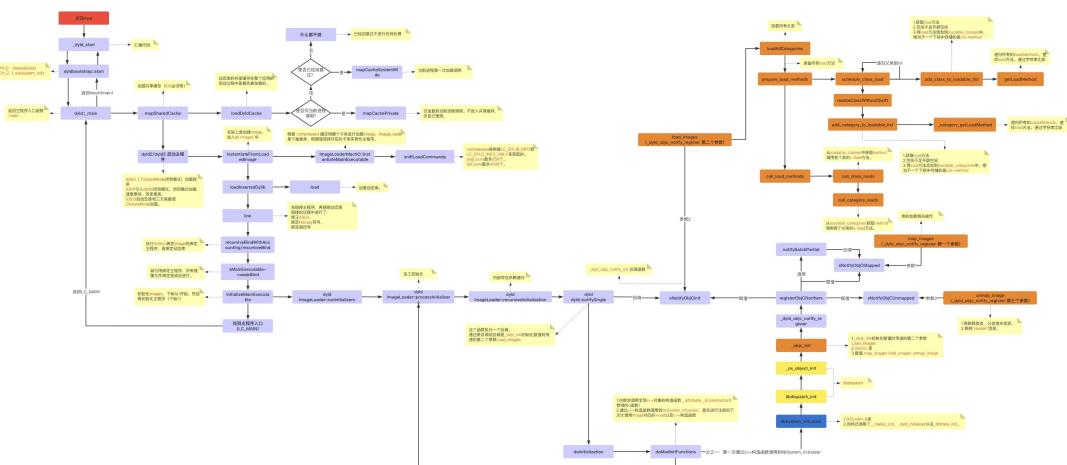
iOS的app启动过程

- iOS的app启动过程

 - 概述

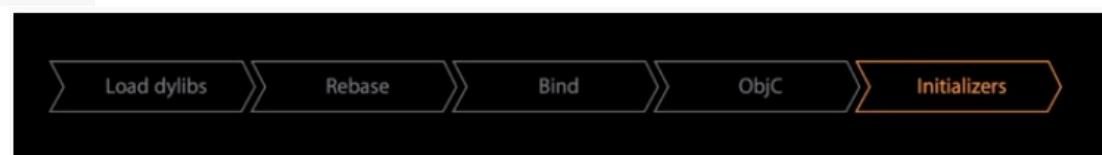


- 详细

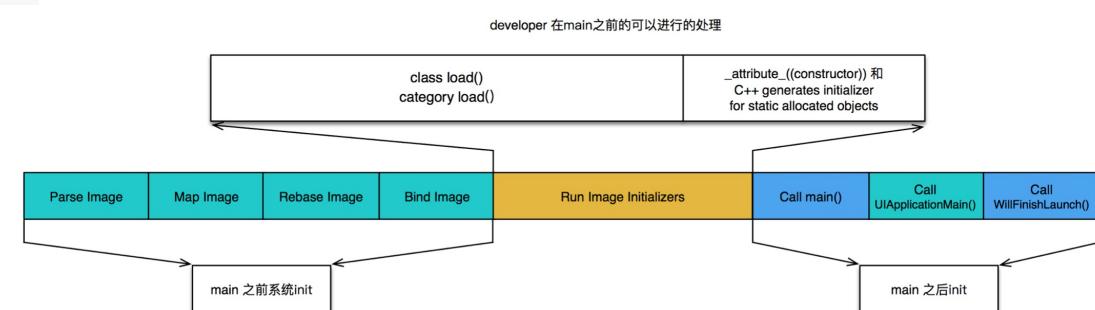


- iOS的app启动的不同阶段

 - Pre-main 阶段



 - main 阶段



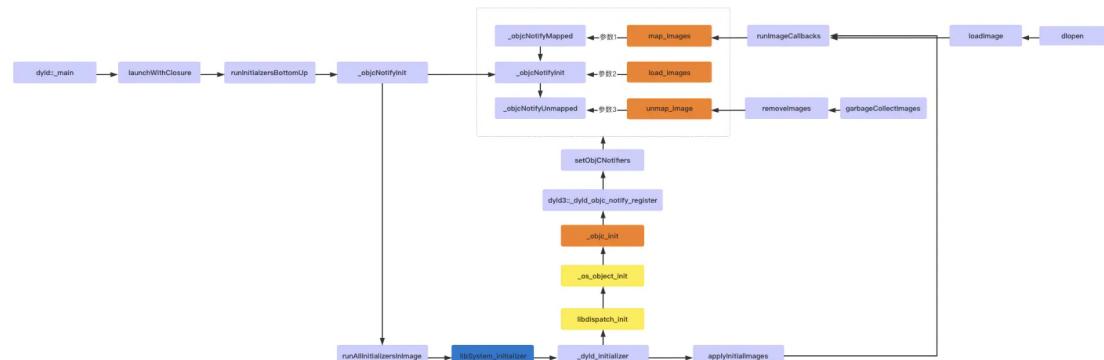
- iOS的app启动调用函数

◦

dyld加载过程

- dyld加载过程

◦ 图



◦ 文字版

- **DYLD** 动态链接器：记载所有库和可执行文件。
- **DYLD** 加载流程：
 - 系统内核调用 `_dyld_start`
 - 重定位 `DYLD` (`rebaseDyld`)
 - 初始化 `DYLD` (`_subsystem_init`)
 - 调用 `dyld main` 函数 (`dyld::main`) :
 - 加载共享缓存 (`mapSharedCache`)
 - 实际调用 `loadDyldCache` 分为三种情况
 - 仅加载到当前进程调用 `mapCachePrivate`。不放入共享缓存，仅自己使用。
 - 已经加载过不进行任何处理。
 - 当前进程第一次加载调用 `mapCacheSystemWide`
 - `dyld2/dyld3` (`ClosureMode` 闭包模式) 加载程序 (`iOS11` 引入 `dyld3` 闭包模式，闭包模式加载速度更快，效率更高。`iOS13` 后 动态库和三方库都使用 `ClosureMode` 加载。) :
 - `dyld3` :
 - 找到/创建 `mainClosure`
 - 通过 `launchWithClosure` 启动主程序，成功后返回 `result` (主程序入口 `main`)。逻辑和 `dyld2` 启动主程序逻辑基本相同。
 - `dyld2` : 启动主程序
 - 实例化主程序 `instantiateFromLoadedImage` (实际上是创建 `image`)
 - 调用 `sniffLoadCommands` 生成相关信息，比如 `compressed`。根据 `compressed` 来确定使用哪个类来实例化。
 - `compressed` 是根据 `LC_DYLIB_INFO` 和 `LC_DYLD_INFO_ONLY` 来获取的。
 - `segCount` 最多 256 个。
 - `LibCount` 最多 4096 个。
 - 实例化生成 `image`，加入 `all_images` 中。
 - 插入&加载动态库 `loadInsertedDylib`
 - 根据上下文初始化配置调用 `load` 加载动态库。
 - 链接主程序和链接插入动态库 (`link`，主程序链接在前)
 - 修正 `ASLR`、绑定 `NoLazy` 符号、绑定弱符号
 - 初始化主程序 `initializeMainExecutable` (核心方法)
 - 初始化 `images`，下标从 1 开始，然后再初始化主程序 (下标 0) 调用 `dyld ImageLoader::runInitializers`:
 - `dyld ImageLoader::processInitializers`:
 - `dyld ImageLoader::recursiveInitialization`:
 - `dyld dyld::notifySingle`:
 - 这个函数执行一个回调。
 - 通过断点调试回调是 `_objc_init` 初始化赋值时传递的第二个参数 `Load_images`:
 - `Load_images` 中调用了 `call_load_methods` 函数
 - `call_class_loads`：调用各个类的 `+ load` 方法。
 - `call_category_loads`：调用各个分类的 `+ load` 方法。
 - `doInitialization`
 - 最终会调用到 `doModInitFunctions`
 - 内部会调用全局 `c++` 对象的构造函数 (`attribute((constructor))` 修饰的 `c` 函数)
 - 会首先调用 `libSystem_initializer` 构造函数进行回调的注册。
 - 回调有三个参数 (`map_images`、`load_images`、`unmap_image`)
 - `map_images` 进行类的加载，在回调函数注册后就立马调用。
 - `load_images` 在 `notifySingle` 循环中调用。
 - `unmap_image` 在异常/回收/检查镜像文件的时候调用。
 - 找到主程序入口 `LC_MAIN`，然后返回主程序 (`main`)。
 - `load`、`C++` 构造函数、`main` 调用总结：
 - `Dyld` 初始化 `image` 是按 `Link Binary With Libraries` 顺序逐个初始化的，从下标 1 开始，最后再初始化主程序 (下标 0)。可以理解为是按 `image` 进行分组的。
 - `image` 内部是先加载所有类的 `+ load`，再加载分类的 `+ load`，最后加载 `C++` 全局构造函数。（类 `load` -> 分类 `load` -> `C++` 构造函数）。`+load` 是 `objc` 中调用的，`C++` 全局构造函数是在 `dyld` 中调用的。(在不考虑二进制重排等的优化下，`image` 内部的顺序默认是按 `Compile Sources` 中顺序进行的)。
 - `main` 函数是在 `dyld` 返回入口函数 (`main`) 之后才调用的。

• dyld2 vs dyld3

◦

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 23:19:48

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 \approx 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
 - \approx PIE = Position-Independent Executable
 - 对应的 Mach-O 中有个 flag 是：MH_PIE
 - \approx ASLR

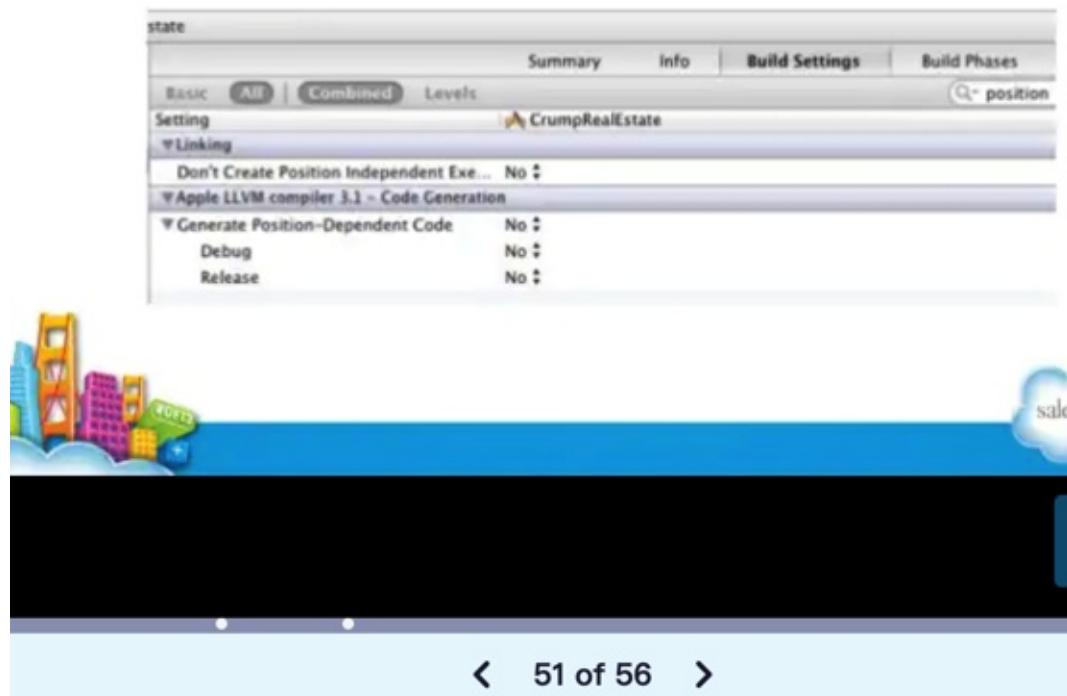
ASLR

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

参考：

Enable ASLR in your app

- ASLR: Address Space Layout Randomization



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 together

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ASLR，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

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 16:44:05

Mach-O格式

Mach-O vs ELF

MACH-O FILE FORMAT VS. EXECUTABLE AND LINKABLE FORMAT(ELF)

| Mach-O... | Is ELF's.. |
|-------------------------|--------------------|
| Segment | Section |
| Section | N/A |
| /usr/lib/dyld | /usr/bin/ld |
| dylib (dynamic library) | so (Shared object) |



Mac OS X and iOS Internals

Jonathan Levin - RSA 2015
<http://newosxbook.com/articles/CodeSigning.pdf>

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 16:00:21

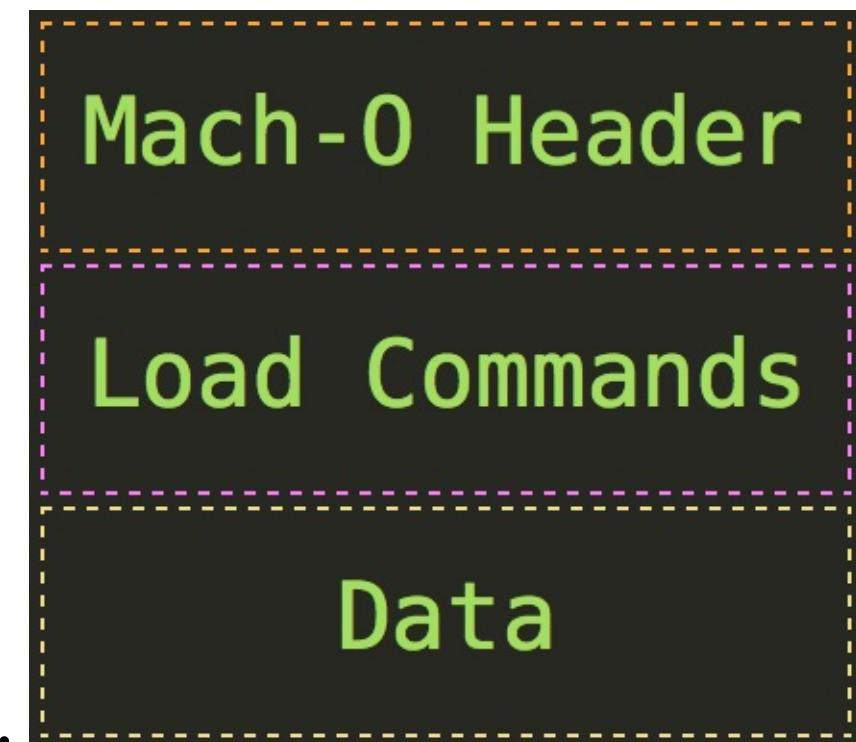
Mach-O结构概述

- 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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 23:01:40

Mach-O结构图

概览



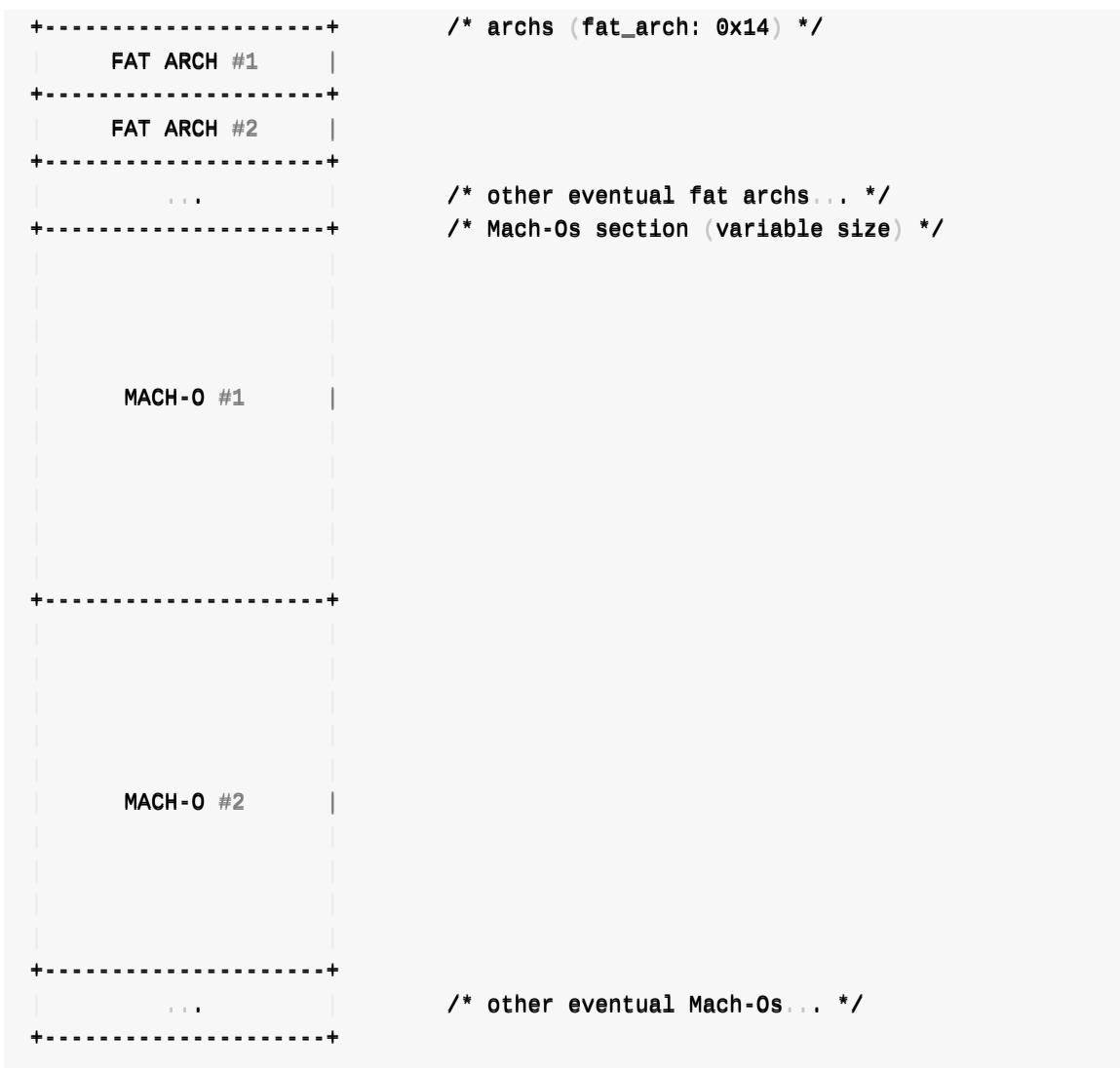
普通单架构 vs FAT多架构

- 普通：单架构 = Mach-O文件

-
- 特殊：多架构= **FAT** =Universal通用文件

-
- 文字版

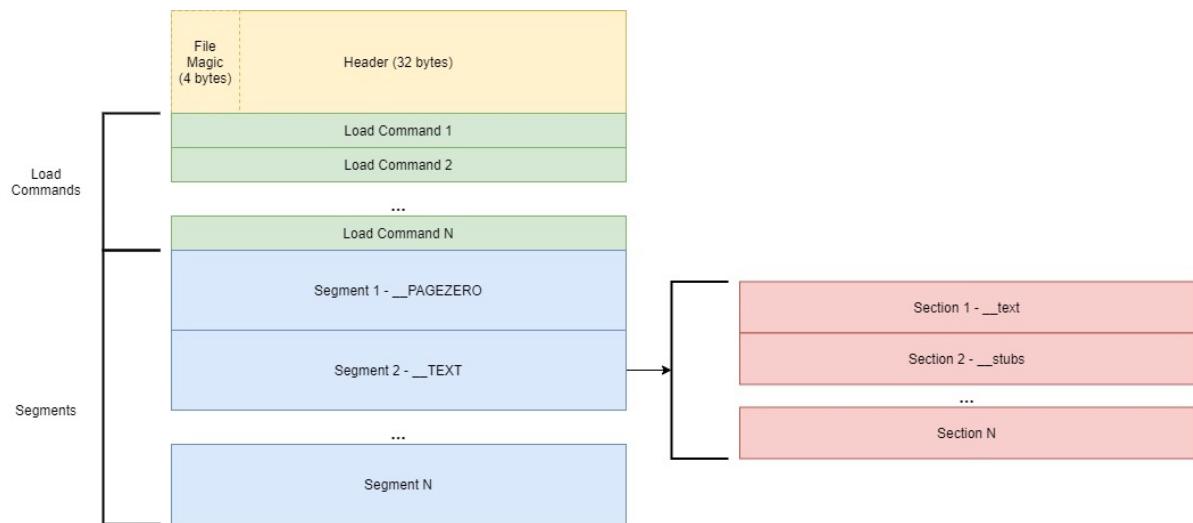
```
+-----+      /* header (fat_header: 0x8) */  
|  
|   FAT HEADER  
|  
|-----|
```



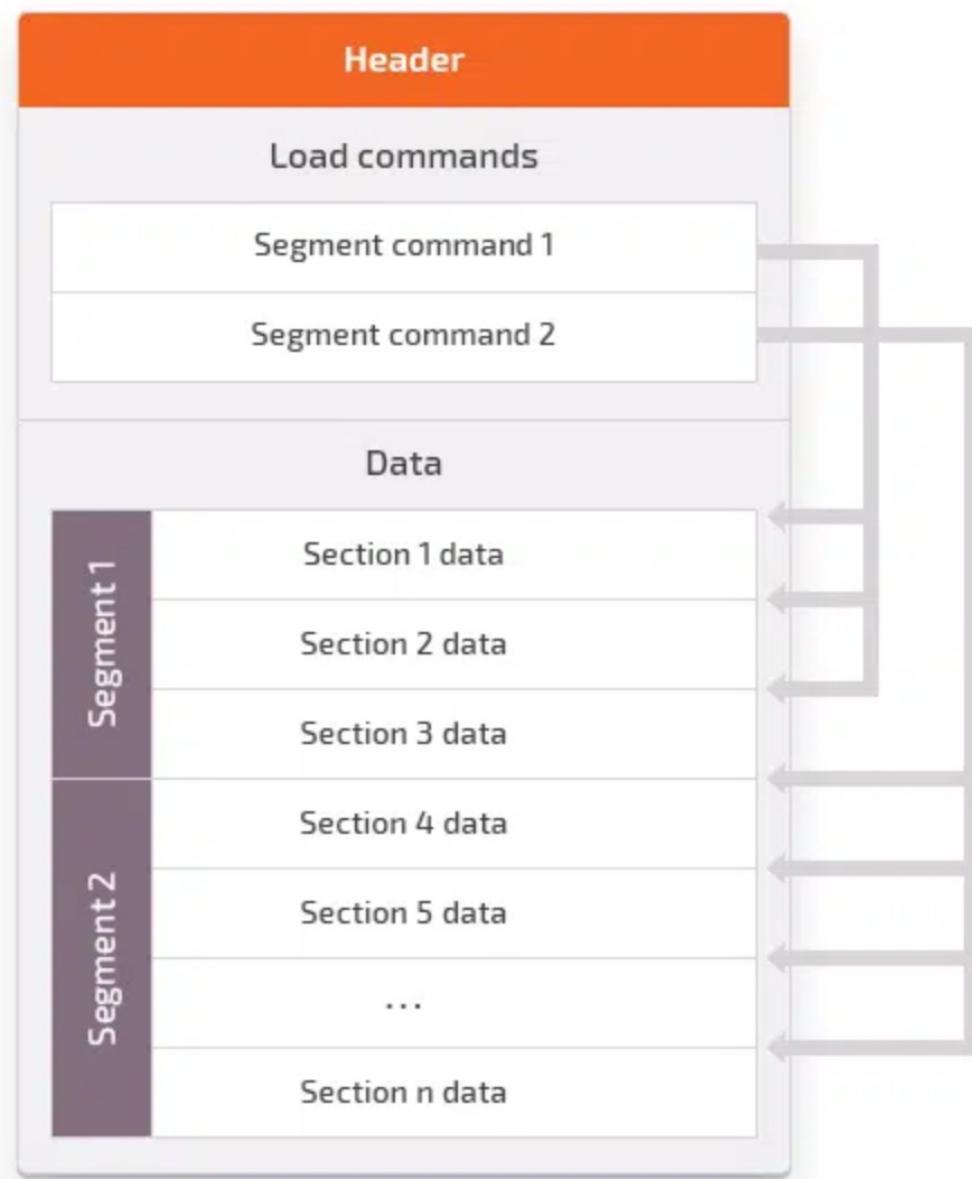
详解

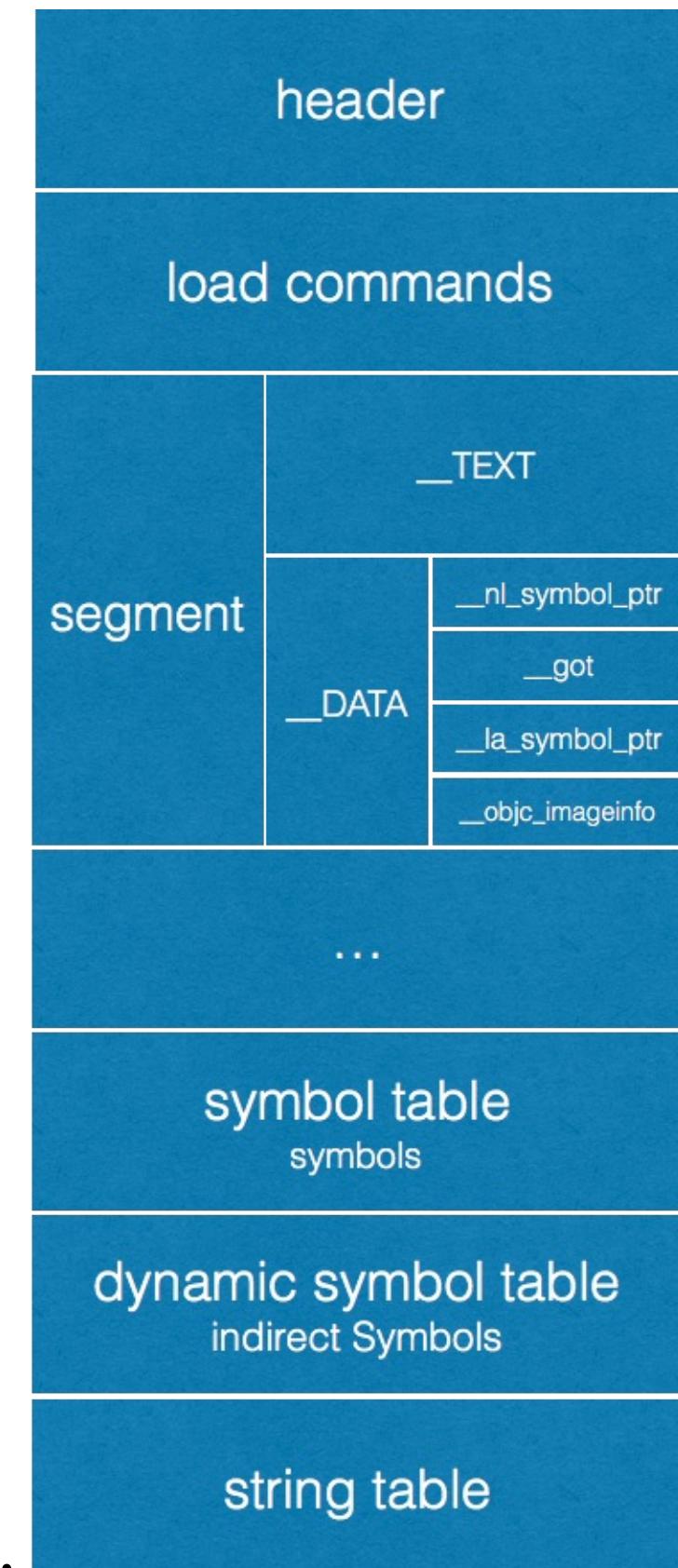
- 带字段的Mach-O结构图

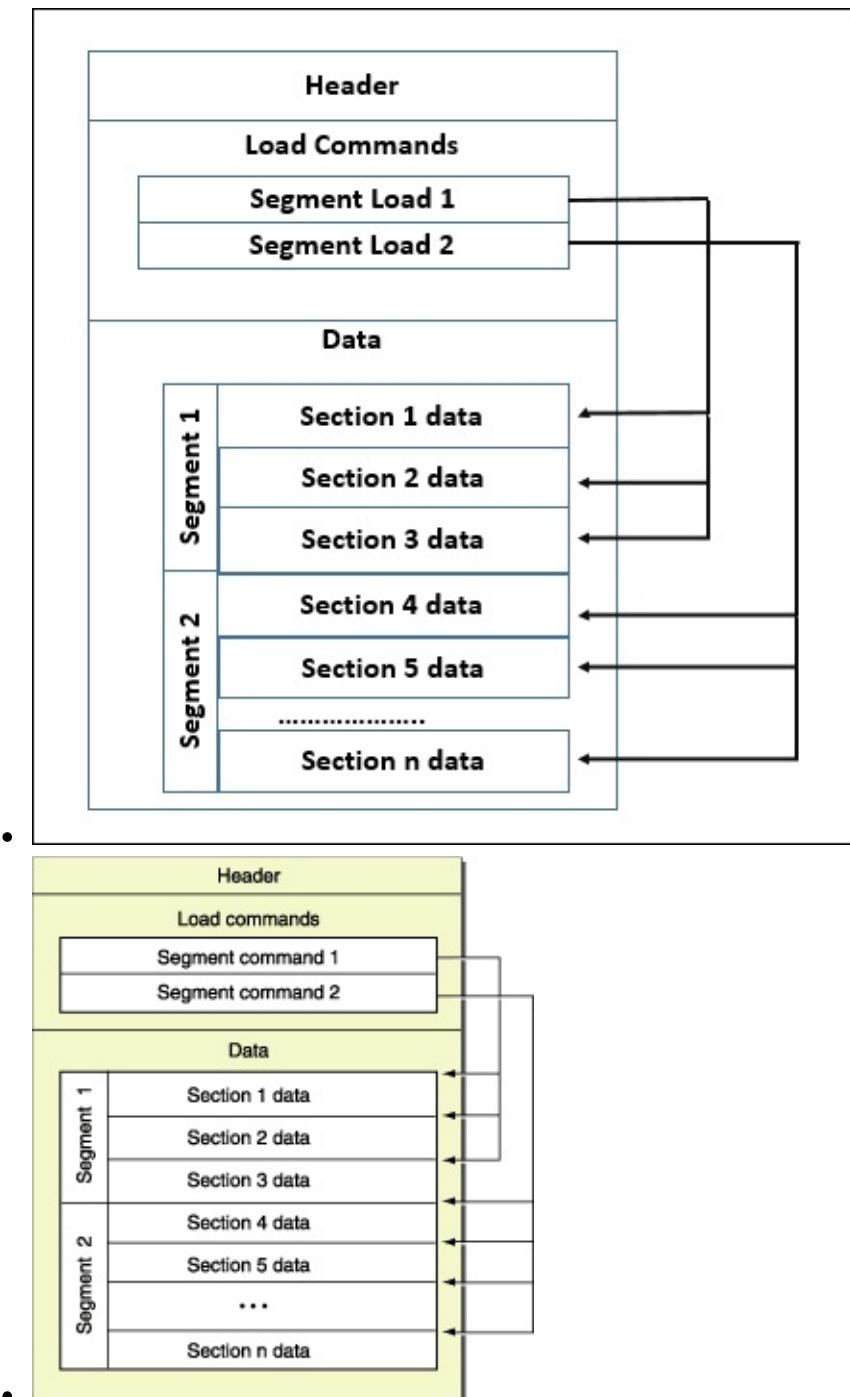
◦



MACH-O FILE FORMAT BASIC STRUCTURE







crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 17:03:08

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 23:01:36

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 command
 - 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   cpusubtype;
    cpu_subtype_t cpusubtype;
    uint32_t      filetype;
    uint32_t      ncmds;
    uint32_t      sizeofcmds;
    uint32_t      flags;
};


```

- 详细定义

源码定义：

```

struct mach_header {
    uint32_t      magic;          /* mach magic number identifier */
    cpu_type_t   cpusubtype;    /* machine 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) */

struct mach_header_64 {
    uint32_t      magic;          /* mach magic number identifier */
    cpu_type_t   cpusubtype;    /* machine 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 0xcfffaedfe /* 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   0xcfffaedfe /* NXSwapInt(MH_MAGIC_64) */
```

->

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:52:31

cputype和cpusubtype

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:54:29

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

HEADER: FILE TYPES & FLAGS

```

/* 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 */

/* 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
                      statically 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. */
...

```

- 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 arbitrary 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 */

```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 15:55:00

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_PREBOUND 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

HEADER: FILE TYPES & FLAGS

What we're focused on

```
/* 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 */
```

```
/* 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. */
...
```

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 statically
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
definitions 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`

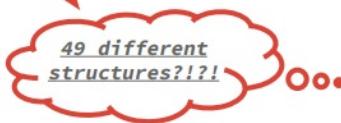
- local of info to split segments
- LC_REEXPORT_DYLIB = 0x1f | LC_REQ_DYLD = 0x8000001f
 - load and re-export dylib
- LC_LAZY_LOAD_DYLIB = 0x20
 - delay load of dylib until first use
- LC_ENCRYPTION_INFO = 0x21
 - encrypted segment information
- LC_DYLD_INFO = 0x22
 - compressed dyld information
- LC_DYLD_INFO_ONLY = 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

LOAD COMMANDS

49 different load commands...



... eh, more like 30

`linkedit_data_command:`

- `LC_CODE_SIGNATURE`
- `LC_SEGMENT_SPLIT_INFO`
- `LC_FUNCTION_STARTS`
- `LC_DYLIB_CODE_SIGN_DRS`
- `LC_LINKER_OPTIMIZATION_HINT`

```
#define LC_SEGMENT 0x1 /* segment of this file to be mapped */
#define LC_SEGMENT_64 0x19 /* 64-bit segment of this file to be mapped */
#define LC_SYMTAB 0x2 /* link-edit stab symbol table info */
#define LC_DYSYMTAB 0xb /* dynamic link-edit symbol table info */
#define LC_LOAD_DYLIB 0xc /* load a dynamically linked shared library */
#define LC_CODE_SIGNATURE 0x1d /* local of code signature */
...
```

```
/*
 * 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... 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.)... 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...
 */

struct load_command {
    uint32_t cmd; /* type of load command */
    uint32_t cmdsize; /* total size of command in bytes */
};
```

•

- 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, payload 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

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 17:04:15

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

| | |
|-----------------------------|---|
| <code>LC 09: LC_UUID</code> | <code>UUID: F1FCF15A-6465-31F0-9300-5BA1B8F91017</code> |
|-----------------------------|---|

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 */  
};
```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 17:18:48

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

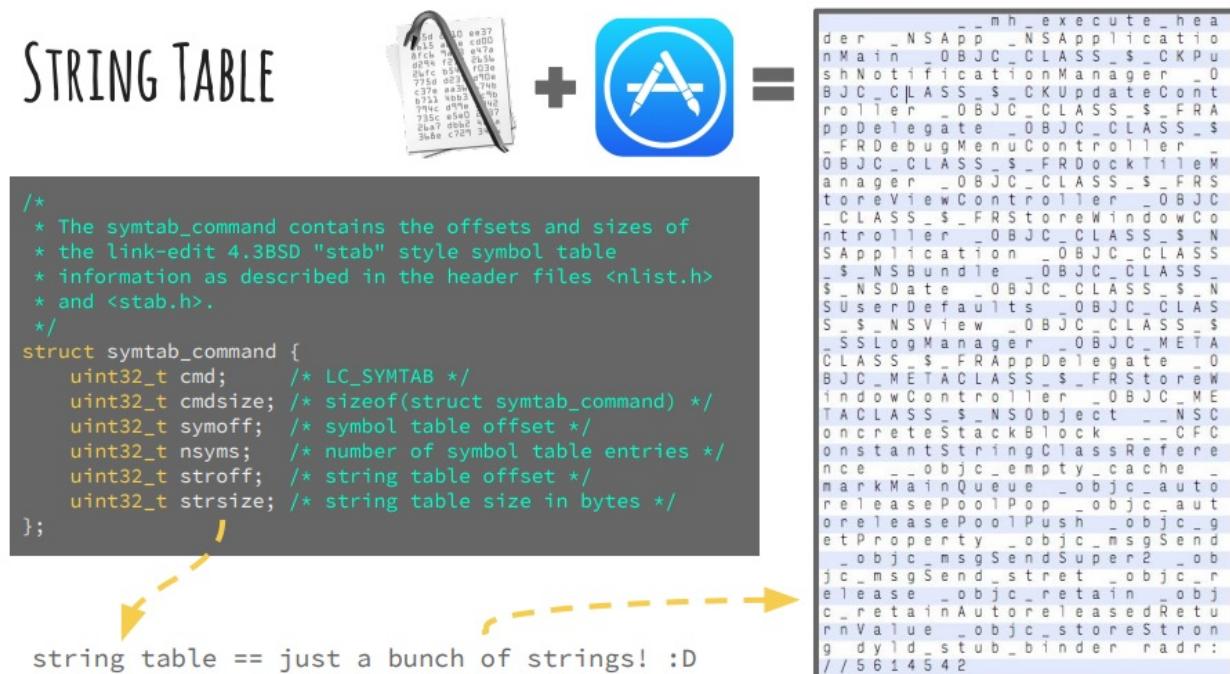
```
/*
 * The 64-bit segment load command indicates that a part of this file is to be
 * mapped into a 64-bit task's address space. If the 64-bit segment has
 * sections then section_64 structures directly follow the 64-bit segment
 * command and their size is reflected in cmdsize.
 */
struct segment_command_64 { /* 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 */
};
```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 17:18:58

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 17:27:14

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 .

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 17:13:14

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](#).

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 17:10:17

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

▼ Load Commands

LC_SEGMENT_64 (_PAGEZERO)

► **LC_SEGMENT_64 (_TEXT)**

► **LC_SEGMENT_64 (_DATA)**

LC_SEGMENT_64 (_LINKEDIT)

LC_DYLD_INFO_ONLY

LC_SYMTAB

LC_DYSYMTAB

LC_LOAD_DYLINKER

LC_UUID

LC_VERSION_MIN_IPHONEOS

LC_SOURCE_VERSION

LC_MAIN

LC_LOAD_DYLIB (libc++.1.dylib)

LC_LOAD_DYLIB (libiconv.2.dylib)

LC_LOAD_DYLIB (libicucore.A.dylib)

LC_LOAD_DYLIB (libresolv.9.dylib)

LC_LOAD_DYLIB (libsqLite3.dylib)

LC_LOAD_DYLIB (libstdc++.6.dylib)

LC_LOAD_DYLIB (libxml2.2.dylib)

LC_LOAD_DYLIB (libz.1.dylib)

LC_LOAD_WEAK_DYLIB (AVFoundation)

LC_LOAD_DYLIB (Accelerate)

LC_LOAD_DYLIB (AddressBook)

LC_LOAD_DYLIB (AssetsLibrary)

LC_LOAD_DYLIB (AudioToolbox)

LC_LOAD_DYLIB (CENetwork)

- 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

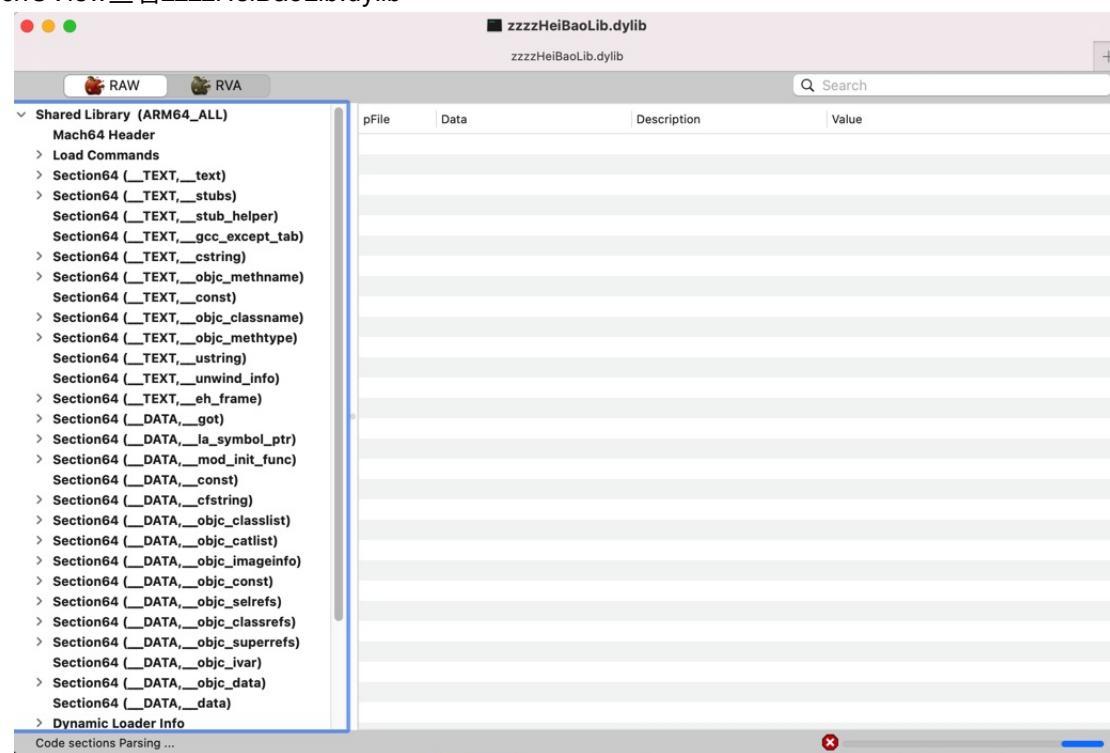
举例

- 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  0x00000037B  __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  0x000000BD8  __DATA      __got
0x100BBBBE0  0x000002628  __DATA      __la_symbol_ptr
0x100BBE208  0x000000070  __DATA      __mod_init_func
0x100BBE280  0x0001CEE0  __DATA      __const
0x100BDB160  0x00039CA0  __DATA      __cfcstring
0x100C14E00  0x00002B00  __DATA      __objc_classlist
0x100C17900  0x000000A0  __DATA      __objc_nlclslist
0x100C179A0  0x000000680  __DATA      __objc_catlist
0x100C18020  0x0000000D0  __DATA      __objc_nlcatlist
0x100C180F0  0x000000638  __DATA      __objc_protolist
0x100C18728  0x000000008  __DATA      __objc_imageinfo
0x100C18730  0x001252F8  __DATA      __objc_const
0x100D3DA28  0x000150B0  __DATA      __objc_selrefs
0x100D52AD8  0x000000150  __DATA      __objc_protorefs
0x100D52C28  0x00002A38  __DATA      __objc_classrefs
0x100D55660  0x0000019F8  __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 |
|-------------------------------|--|
| <code>__text</code> | The compiled machine code for the executable |
| <code>__const</code> | The general constant data for the executable |
| <code>__cstring</code> | Literal string constants (quoted strings in source code) |
| <code>__picsymbol_stub</code> | 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

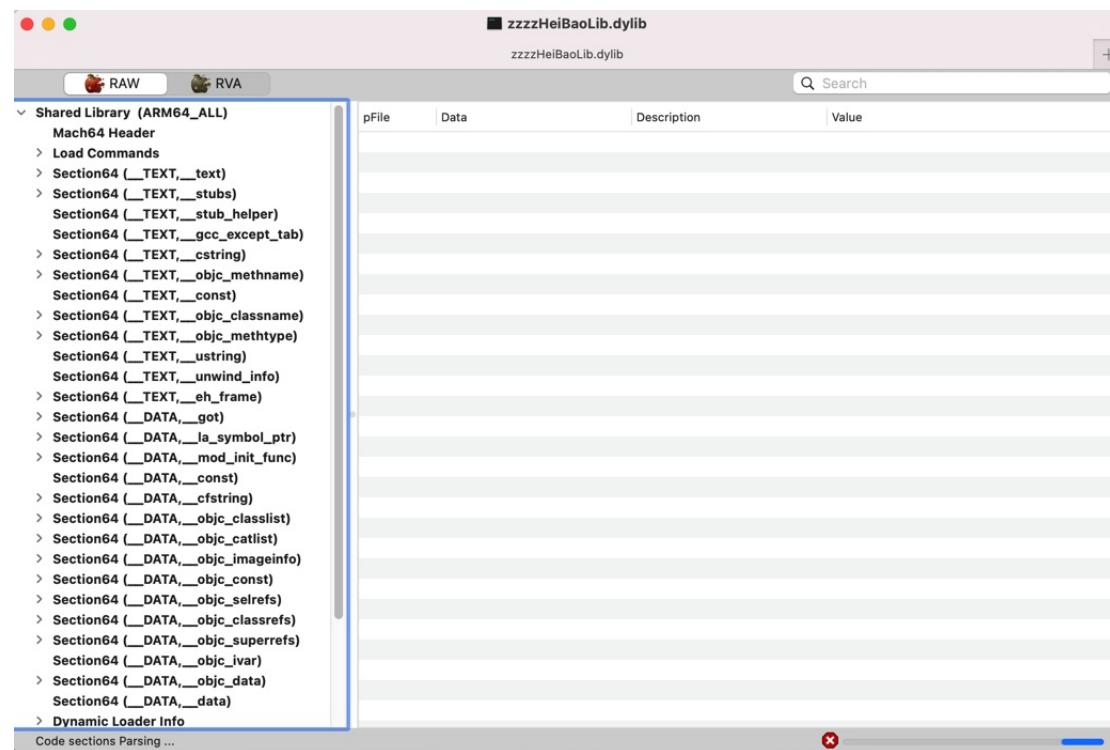
- `__TEXT, __objc_methname`

- `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_RACCompon`
- `__TEXT,__unwind_info`
- `__TEXT,__ustring`

举例

- MachOView查看
 - `zzzzHeiBaoLib.dylib`



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 22:09:17

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)

| | Offset | Data | Description | Value |
|--|----------|---------------------|--------------------------|------------|
| Executable (ARM64_ALL) | 000000B0 | 5F5F7465787400000.. | Section Name | __text |
| Mach64 Header | 000000C0 | 5F5F545585400000.. | Segment Name | __TEXT |
| > Load Commands | 000000D0 | 00000001000043D0 | Address | 4294984656 |
| > LC_SEGMENT_64 (__PAGEZERO) | 000000D8 | 00000000000087B54 | Size | 752468 |
| > LC_SEGMENT_64 (__TEXT) | 000000E0 | 000043D0 | Offset | 17360 |
| > Section64 Header (__stubs) | 000000E4 | 00000002 | Alignment | 4 |
| > Section64 Header (__objc_methlist) | 000000E8 | 00000000 | Relocations Offset | 0 |
| > Section64 Header (__const) | 000000EC | 00000000 | Number of Relocations | 0 |
| > Section64 Header (__gcc_except_tab) | 000000F0 | 00000400 | Flags | |
| > Section64 Header (__objc_methname) | | 00000000 | S_REGULAR | |
| > Section64 Header (__cstring) | | 00000000 | S_ATTR_PURE_INSTRUCTIONS | |
| > Section64 Header (__oslogstring) | | 00000000 | S_ATTR_SOME_INSTRUCTIONS | |
| > Section64 Header (__objc_classname) | | | | |
| > Section64 Header (__objc_methtype) | | | | |
| > Section64 Header (__dlopen_cstrs) | | | | |
| > Section64 Header (__info.plist) | | | | |
| > Section64 Header (__ unwind_info) | | | | |
| > LC_SEGMENT_64 (__DATA_CONST) | | | | |
| > LC_SEGMENT_64 (__DATA) | | | | |
| > LC_SEGMENT_64 (__LINKEDIT) | | | | |
| ??? (unsupported) | | | | |
| ??? (unsupported) | | | | |
| LC_SYMTAB | | | | |
| LC_DYSYMTAB | | | | |
| LC_LOAD_DYLINKER | | | | |
| LC_UUID | | | | |
| ??? (unsupported) | | | | |
| LC_SOURCE_VERSION | | | | |
| LC_MAIN | | | | |
| LC_LOAD_WEAK_DYLIB (Accounts) | | | | |
| LC_LOAD_DYLIB (MobileKeyBag) | | | | |
| LC_LOAD_DYLIB (CoreDV) | | | | |
| LC_LOAD_DYLIB (libSystem.B.dylib) | | | | |
| LC_LOAD_DYLIB (libMobileGestalt.dylib) | | | | |
| LC_LOAD_DYLIB (BaseBoard) | | | | |
| LC_LOAD_DYLIB (libsqlite3.dylib) | | | | |
| LC_LOAD_WEAK_DYLIB (CoreAnalytics) | | | | |
| LC_LOAD_DYLIB (CoreTelephony) | | | | |
| LC_LOAD_DYLIB (AppSupport) | | | | |
| LC_LOAD_DYLIB (ApplIdAuthSupport) | | | | |
| LC_LOAD_DYLIB (AssertionServices) | | | | |
| LC_LOAD_DYLIB (AuthKit) | | | | |
| LC_LOAD_DYLIB (CommonUtilities) | | | | |
| LC_LOAD_DYLIB (SoftLinking) | | | | |
| LC_LOAD_DYLIB (Foundation) | | | | |

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

| | File | Data LO | Data HI | Value |
|--|----------|---------------------|-------------------------|-------------------|
| Executable (ARM64_ALL) | 000000B0 | FF 83 00 D1 FD 7B.. | FD 43 00 91 88 00 B0 |{...C..... |
| Mach64 Header | 000000C0 | 00 29 42 F9 E0 23.. | 68 00 00 B0 01 95 40 F9 |B,...h,...@.. |
| > Load Commands | 000000D0 | E0 03 00 91 3D E0.. | 40 00 00 B4 1F 08 00 B9 |=,...@,... |
| > LC_SEGMENT_64 (__PAGEZERO) | 000000D8 | 00000001000043D0 | | |
| > LC_SEGMENT_64 (__TEXT) | 000000E0 | 000043D0 | | |
| > Section64 Header (__stubs) | 000000E4 | F0 78 41 A9 FF 83.. | C0 03 5F D6 FD 7B BF A9 | .{A.....,..{.. |
| > Section64 Header (__objc_methlist) | 000000E8 | F0 03 00 91 A8 08.. | 08 70 47 F9 1F 05 00 B1 |){,..G,.. |
| > Section64 Header (__const) | 000000EC | A1 00 00 54 A8 08.. | 00 79 47 F9 FD 7B C1 A9 | ..T,...,yG,..{, |
| > Section64 Header (__gcc_except_tab) | 000000F0 | 00004430 | | |
| > Section64 Header (__objc_methname) | 000000F4 | 46 E8 02 14 A8 08.. | 00 E8 3B 91 A1 49 78 10 | F.....,..{,..Ix, |
| > Section64 Header (__cstring) | 000000F8 | 00004446 | | |
| > Section64 Header (__oslogstring) | 000000FC | 1F 28 03 D5 A8 DF.. | F7 FF 17 FD 7B BF A9 |,..{,.. |
| > Section64 Header (__objc_classname) | 00000100 | 00004456 | | |
| > Section64 Header (__objc_methtype) | 00000104 | F0 78 C1 A8 2C E0.. | FA 67 BB A9 F0 5F 01 A9 | ..,{.,..,G,..,.. |
| > Section64 Header (__dlopen_cstrs) | 00000108 | 00004448 | | |
| > Section64 Header (__info.plist) | 0000010C | F5 57 02 A9 F4 4F.. | F0 78 04 A9 FD 03 01 91 | ,W,...O,..{,.. |
| > Section64 Header (__ unwind_info) | 00000110 | 00004449 | | |
| > Section64 Header (__LINKEDIT) | 00000114 | F4 03 00 AA E0 03.. | 16 E0 02 94 F3 03 00 AA |,..K,.. |
| > LC_SEGMENT_64 (__DATA_CONST) | 00000118 | 0000444A | | |
| > LC_SEGMENT_64 (__DATA) | 0000011C | 68 00 00 B0 01 99.. | 00 E0 02 94 FD 03 1D AA | h.....@.. |
| > LC_SEGMENT_64 (__LINKEDIT) | 00000120 | 0000444B | | |
| > Section64 Header (__objc_protolist) | 00000124 | 29 E0 02 94 F6 03.. | 60 00 00 B0 01 90 40 F9 |).....,..h,...@.. |
| > Section64 Header (__objc_imageinfo) | 00000128 | 0000444C | | |
| > Section64 Header (__objc_const) | 0000012C | 07 E0 02 94 FD 03.. | 23 E0 02 94 F5 03 00 AA |,..#,... |
| > Section64 Header (__objc_srefers) | 00000130 | 0000444D | | |
| > Section64 Header (__objc_protorefs) | 00000134 | E0 03 16 AA 14 E0.. | 68 00 00 B0 01 A1 40 F9 |,..h,...@.. |
| > Section64 Header (__objc_clasrefs) | 00000138 | 0000444E | | |
| > Section64 Header (__objc_superrrefs) | 00000142 | E0 03 13 AA FE DF.. | F0 83 1D AA E0 02 94 |,..h,...@.. |
| > Section64 Header (__objc_var) | 00000146 | 0000444F | | |
| > Section64 Header (__objc_data) | 00000150 | F5 03 00 AA 68 08.. | 01 A5 48 F9 E0 03 13 AA |,..h,...@.. |
| > Section64 Header (__objc_intobj) | 00000154 | 00004500 | | |
| > Function Starts | 00000158 | F7 DF 02 94 FD 03.. | 13 E0 02 94 F7 03 00 AA |,.. |
| > Symbol Table | 00000162 | 60 00 00 B0 01 A9.. | E0 03 13 AA FD 02 94 | h.....@.. |
| Data in Code Entries | 00000166 | 00004510 | | |
| > Dynamic Symbol Table | 00000170 | 00004520 | | |
| > String Table | 00000174 | 00004530 | | |
| Code Signature | 00000178 | 00004540 | | |
| > Section64 Header (__objc_srefers) | 00000182 | 00004544 | | |
| > Section64 Header (__objc_protorefs) | 00000186 | 60 00 00 B0 01 B1.. | E0 03 13 AA E0 02 94 | h.....@.. |
| > Section64 Header (__objc_clasrefs) | 00000190 | 00004548 | | |
| > Section64 Header (__objc_superrrefs) | 00000194 | F0 03 1D AA FC DF.. | F9 03 00 AA EE DF 02 94 |,.. |
| > Section64 Header (__objc_var) | 00000198 | 00004550 | | |
| > Section64 Header (__objc_data) | 00000202 | 79 02 00 B5 6B 08.. | 01 85 48 F9 E0 03 14 AA | y...h,...@,.. |
| > Section64 Header (__objc_intobj) | 00000206 | 00004558 | | |
| > Function Starts | 00000210 | E2 03 16 AA E3 03.. | E4 03 17 AA D4 DF 02 94 |,.. |
| > Symbol Table | 00000214 | 00004559 | | |
| Data in Code Entries | 00000218 | F0 03 1D AA F0 DF.. | F9 03 00 AA 68 00 00 B0 |,..h,.. |
| > Dynamic Symbol Table | 00000222 | 0000455A | | |
| > String Table | 00000226 | 01 B9 40 F9 E0 03.. | E2 03 19 AA E3 03 15 AA | ..@,..,.. |
| Code Signature | 00000230 | 0000455B | | |
| > Section64 Header (__objc_srefers) | 00000234 | CB DF 02 94 E0 03.. | D8 DF 02 94 E0 03 18 AA |,.. |
| > Section64 Header (__objc_protorefs) | 00000238 | 0000455C | | |
| > Section64 Header (__objc_clasrefs) | 00000242 | D9 DF 02 94 E0 03.. | D7 DF 02 94 E0 03 16 AA |,.. |
| > Section64 Header (__objc_var) | 00000246 | 0000455D | | |
| > Section64 Header (__objc_data) | 00000250 | D5 DF 02 94 E0 03.. | D3 DF 02 94 E0 03 13 AA |,.. |
| > Section64 Header (__objc_intobj) | 00000254 | 0000455E | | |
| > Function Starts | 00000258 | FD 78 44 A9 F4 4F.. | F6 57 42 A9 F8 5F 41 A9 | .D..OC,..WB,..A. |
| > Symbol Table | 00000262 | 0000455F | | |
| Data in Code Entries | 00000266 | FA 67 C5 A8 CC DF.. | FF 03 02 D1 F8 5F 04 A9 | .g,.....,.. |
| > Dynamic Symbol Table | 00000270 | 00004560 | | |
| > String Table | 00000274 | F5 57 05 A9 F4 4F.. | 78 07 A9 FD C3 01 91 | .W,...O,..{,.. |
| Code Signature | 00000278 | 00004561 | | |
| > Section64 Header (__objc_srefers) | 00000282 | F4 03 03 AA F5 03.. | E3 03 02 AA C5 DF 02 94 |,.. |
| > Section64 Header (__objc_protorefs) | 00000286 | 00004562 | | |
| > Section64 Header (__objc_clasrefs) | 00000290 | F3 03 00 AA E6 03.. | C2 DF 02 94 F4 03 00 AA |,.. |
| > Section64 Header (__objc_var) | 00000294 | 00004563 | | |
| > Section64 Header (__objc_data) | 00000298 | 60 00 00 B0 16 BD.. | E1 03 16 AA A8 DF 02 94 | h.....@,.. |
| > Section64 Header (__objc_intobj) | 00000302 | 00004564 | | |
| > Function Starts | 00000306 | F3 03 1D AA C4 DF.. | F7 03 00 AA 68 00 00 B0 |,..h,.. |
| > Symbol Table | 00000310 | 00004565 | | |
| Data in Code Entries | 00000314 | 01 C1 40 F9 E0 03.. | E2 03 17 AA A0 DF 02 94 | ..@,.....,..x,.. |
| > Dynamic Symbol Table | 00000318 | 00004566 | | |
| > String Table | 00000322 | F8 03 00 AA E6 03.. | AF DF 02 94 78 07 00 34 |,.. |
| Code Signature | 00000326 | 00004567 | | |
| > Section64 Header (__objc_srefers) | 00000330 | B5 DF 02 94 F6 03.. | 68 00 00 B0 01 99 40 F9 |,..h,...@,.. |
| > Section64 Header (__objc_protorefs) | 00000334 | 00004568 | | |
| > Section64 Header (__objc_clasrefs) | 00000338 | 00004569 | | |

| | pFile | Data LO | Data HI | Value |
|---|-------|---------|---------|-------|
| 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,__objc_methtype) | | | | |
| > Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__info_plist) | | | | |
| Section64 (__TEXT,__unwind_info) | | | | |
| > Section64 (__DATA,__const,_got) | | | | |
| Section64 (__DATA,__CONST,_const) | | | | |
| > Section64 (__DATA,__CONST,_cstring) | | | | |
| Section64 (__DATA,__OBJC_CLASSNAME) | | | | |
| > Section64 (__TEXT,__objc_classlist) | | | | |
| Section64 (__DATA,__OBJC_CATALOG) | | | | |
| > Section64 (__DATA,__OBJC_PROTOCOL) | | | | |
| Section64 (__DATA,__CONST,_objc_protocol) | | | | |
| Section64 (__DATA,__CONST,_objc_imageninfo) | | | | |
| Section64 (__DATA,__OBJC_CONST) | | | | |
| > Section64 (__DATA,__objc_srefs) | | | | |
| 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 | | | | |
| 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,__objc_methtype) | | | | |
| > Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__info_plist) | | | | |
| Section64 (__TEXT,__unwind_info) | | | | |
| > Section64 (__DATA,__const,_got) | | | | |
| Section64 (__DATA,__CONST,_const) | | | | |
| > Section64 (__DATA,__CONST,_cstring) | | | | |
| Section64 (__DATA,__OBJC_CLASSNAME) | | | | |
| > Section64 (__TEXT,__objc_classlist) | | | | |
| Section64 (__DATA,__OBJC_CATALOG) | | | | |
| > Section64 (__DATA,__OBJC_PROTOCOL) | | | | |
| Section64 (__DATA,__CONST,_objc_protocol) | | | | |
| Section64 (__DATA,__CONST,_objc_imageninfo) | | | | |
| Section64 (__DATA,__OBJC_CONST) | | | | |
| > Section64 (__DATA,__objc_srefs) | | | | |
| 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 | | | | |

- 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)

| | Offset | Data | Description | Value |
|---|--------|------|-------------|-------|
| 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,__objc_methtype) | | | | |
| > Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__info_plist) | | | | |
| Section64 (__TEXT,__unwind_info) | | | | |
| > Section64 (__DATA,__const,_got) | | | | |
| Section64 (__DATA,__CONST,_const) | | | | |
| > Section64 (__DATA,__CONST,_cstring) | | | | |
| Section64 (__DATA,__OBJC_CLASSNAME) | | | | |
| > Section64 (__TEXT,__objc_classlist) | | | | |
| Section64 (__DATA,__OBJC_CATALOG) | | | | |
| > Section64 (__DATA,__OBJC_PROTOCOL) | | | | |
| Section64 (__DATA,__CONST,_objc_protocol) | | | | |
| Section64 (__DATA,__CONST,_objc_imageninfo) | | | | |
| Section64 (__DATA,__OBJC_CONST) | | | | |
| > Section64 (__DATA,__objc_srefs) | | | | |
| 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 | | | | |
| 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,__objc_methtype) | | | | |
| > Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__dlopen_cstrs) | | | | |
| Section64 (__TEXT,__info_plist) | | | | |
| Section64 (__TEXT,__unwind_info) | | | | |
| > Section64 (__DATA,__const,_got) | | | | |
| Section64 (__DATA,__CONST,_const) | | | | |
| > Section64 (__DATA,__CONST,_cstring) | | | | |
| Section64 (__DATA,__OBJC_CLASSNAME) | | | | |
| > Section64 (__TEXT,__objc_classlist) | | | | |
| Section64 (__DATA,__OBJC_CATALOG) | | | | |
| > Section64 (__DATA,__OBJC_PROTOCOL) | | | | |
| Section64 (__DATA,__CONST,_objc_protocol) | | | | |
| Section64 (__DATA,__CONST,_objc_imageninfo) | | | | |
| Section64 (__DATA,__OBJC_CONST) | | | | |
| > Section64 (__DATA,__objc_srefs) | | | | |
| 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 | | | | |

Raw RVA

Executable (ARM64_ALL)

Mach64 Header

Load Commands

Section64 (.TEXT, __text)

Assembly

| Offset | Data | Description | Value |
|----------|----------|------------------------------------|-------|
| 000BBE70 | FFC30001 | sub sp, sp, #0x30 | |
| 000BBE74 | F07B02A0 | stp x29, x30, [sp, #0x20] | |
| 000BBE78 | FD380091 | add x29, sp, #0x20 | |
| 000BBE7C | 1F2003D5 | nop | |
| 000BBE80 | C841C58 | ldr x8, #0x1000f47d8 | |
| 000BBE84 | 080140F9 | ldr x8, [x8] | |
| 000BBE88 | A8B31FF8 | stur x8, [x29, #0xffffffffffff...] | |
| 000BBE8C | 48200052 | movz w8, #0x102 | |
| 000BBE90 | 0808A172 | movk w8, #0x840, ls1 #16 | |
| 000BBE94 | E80300B9 | str w8, [sp] | |
| 000BBE98 | E04300F8 | stur x8, [sp, #4] | |
| 000BBE9C | 2008A210 | adr x8, #0x100000000 | |
| 000BBEA0 | 1F2003D5 | nop | |
| 000BBEA4 | 03A21850 | adr x3, #0x1000ed2e6 | |
| 000BBEA8 | 1F2003D5 | nop | |
| 000BBEAC | E4030091 | mov x4, sp | |
| 000BBE80 | 02020052 | mvz x2, #0x10 | |
| 000BBE84 | B5010052 | mvz w5, #0xc | |
| 000BBE88 | D8000094 | bl #0x1000bc224 | |
| 000BBE8C | A8B35FF8 | ldur x8, [x29, #0xffffffffffff...] | |
| 000BBE90 | 1F2003D5 | nop | |
| 000BBE94 | A9481C58 | ldr x9, #0x1000f47d8 | |
| 000BBE98 | 290140F9 | ldr x9, [x9] | |
| 000BBEC0 | 3F0180E8 | cmp x9, x8 | |
| 000BBED0 | B1000054 | b.ne #0x1000bbe9 | |
| 000BBED4 | F07B02A0 | ldp x29, x30, [sp, #0x20] | |
| 000BBED8 | FFC30091 | add sp, sp, #0x30 | |
| 000BBEDC | C0035FD6 | ret | |
| 000BBEE0 | C5000094 | bl #0x1000bc1f4 | |
| 000BBEE4 | F0380001 | sub sp, sp, #0x20 | |
| 000BBEE8 | F07B01A9 | stp x29, x30, [sp, #0x10] | |
| 000BBEC0 | F0430091 | add x29, sp, #0x10 | |
| 000BBEF0 | E10300A0 | mov x1, x0 | |
| 000BBEF4 | F0030079 | strh wzr, [sp] | |
| 000BBEF8 | 4008A210 | adr x0, #0x10000000 | |
| 000BBEFC | 1F2003D5 | nop | |
| 000BBF00 | A3A11870 | adr x3, #0x1000ed337 | |
| 000BBF04 | 1F2003D5 | nop | |
| 000BBF08 | E4030091 | mov x4, sp | |
| 000BBF0C | 02020052 | mvz w2, #0x10 | |
| 000BBF10 | 45000052 | mvz w5, #0x2 | |
| 000BBF14 | C4000094 | bl #0x1000bc224 | |
| 000BBF18 | F07B01A9 | ldp x29, x30, [sp, #0x10] | |
| 000BBF1C | FF380091 | add sp, sp, #0x20 | |
| 000BBF20 | C0035FD6 | ret | |

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 21:59:32

DATA

__DATA segment的section：

- 概述

- 图

Table 2 Major sections of the __DATA segment

| Section | Description |
|-----------------|--|
| __data | Initialized global variables (for example <code>int a = 1;</code> or <code>static int a = 1;</code>). |
| __const | Constant data needing relocation (for example, <code>char * const p = "foo";</code>). |
| __bss | Uninitialized static variables (for example, <code>static int a;</code>). |
| __common | Uninitialized external globals (for example, <code>int a;</code> 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.

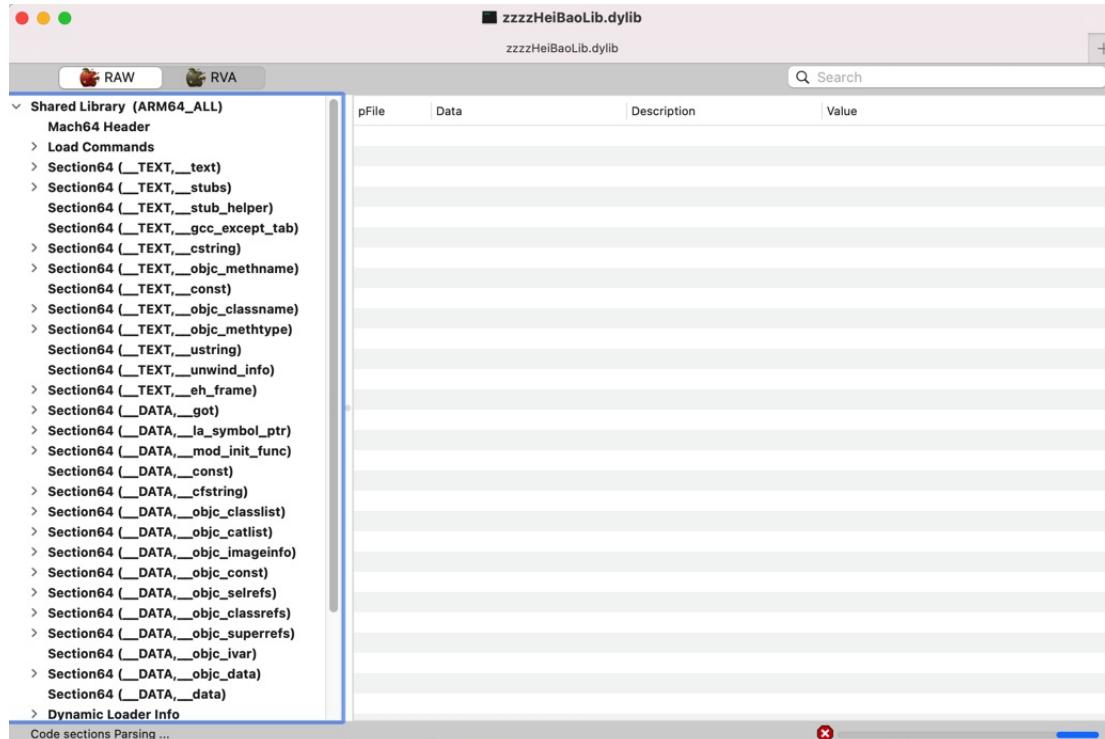
- 放了协议和一些固定了地址（已经初始化）的静态量
- `__DATA,__la_symbol_ptr`
 - Lazy symbol pointers, which are indirect references to functions imported from a different file
 - 详见: [PIC](#)
 - 懒加载的函数指针地址。和 `_stubs` 和 `_stub_helper` 配合使用
- `__DATA,__nl_symbol_ptr`
 - Non-lazy symbol pointers, which are indirect references 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`
 - objct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 command

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|-----------------|
| 000004C8 | 00000019 | Command | LC_SEGMENT_64 |
| 000004C4 | 00000728 | Command Size | 1832 |
| 000004C8 | 5F5F4415441800000000000000000000 | Segment Name | __DATA |
| 000004D0 | 0000000103EBB000 | VM Address | 4360744960 |
| 000004E0 | 000000000003EBB000 | VM Size | 12488704 |
| 000004E8 | 000000000003EBB000 | File Offset | 65777664 |
| 000004F0 | 000000000009F1000 | File Size | 10424320 |
| 000004F8 | 00000007 | Maximum VM Protection | |
| | | 00000001 | VM_PROT_READ |
| | | 00000002 | VM_PROT_WRITE |
| | | 00000004 | VM_PROT_EXECUTE |
| 000004FC | 00000003 | Initial VM Protection | |
| | | 00000001 | VM_PROT_READ |
| | | 00000002 | VM_PROT_WRITE |
| 00000500 | 00000016 | Number of Sections | 22 |
| 00000504 | 00000000 | Flags | |

- 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
- 这个条附属了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

▼ LC_SEGMENT_64 (_DATA)

Section64 Header (_nl_symbol_ptr)
Section64 Header (_got)
Section64 Header (_la_symbol_ptr)
Section64 Header (_mod_init_func)
Section64 Header (_const)
Section64 Header (_cfstring)
Section64 Header (_objc_classlist)
Section64 Header (_objc_nlclslist)
Section64 Header (_objc_catlist)
Section64 Header (_objc_nlcatlist)
Section64 Header (_objc_protolist)
Section64 Header (_objc_imageinfo)
Section64 Header (_objc_const)
Section64 Header (_objc_selrefs)
Section64 Header (_objc_protorefs)
Section64 Header (_objc_classrefs)
Section64 Header (_objc_superrefs)
Section64 Header (_objc_ivar)
Section64 Header (_objc_data)
Section64 Header (_data)
Section64 Header (_bss)
Section64 Header (_common)

LC_SEGMENT_64 (_LINKEDIT)

DATA,la_symbol_ptr

举例

MachOView查看zzzzHeiBaoLib.dylib

| zzzzHeiBaoLib.dylib | | | | |
|--|----------|-------------------------|-------------------------|-----------------|
| | File | Data LO | Data HI | Value |
| > Section64 __TEXT,__cstring) | 0053C2F0 | CC AB 4A 00 00 00 00 00 | D8 AB 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__objc_methname) | 0053C300 | E4 AB 4A 00 00 00 00 00 | F0 AB 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__const) | 0053C310 | 9C AE 4A 00 00 00 00 00 | AB AE 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__objc_classname) | 0053C320 | B4 AE 4A 00 00 00 00 00 | C0 AE 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__objc_methtype) | 0053C330 | CC AE 4A 00 00 00 00 00 | D8 AE 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__unwind_info) | 0053C340 | E4 AE 4A 00 00 00 00 00 | F0 AE 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __TEXT,__eh_frame) | 0053C350 | C8 A9 4A 00 00 00 00 00 | 04 AA 4A 00 00 00 00 00 | ..J.....J.... |
| > Section64 __DATA,__got) | 0053C360 | 10 AA 4A 00 00 00 00 00 | 1C AA 4A 00 00 00 00 00 | ..J.....J.... |
| Non-Lazy Symbol Pointers | 0053C370 | 28 AA 4A 00 00 00 00 00 | 34 AA 4A 00 00 00 00 00 | (.J....4.J....) |
| < Section64 __DATA,la_symbol_ptr) | 0053C380 | 40 AA 4A 00 00 00 00 00 | D4 A9 4A 00 00 00 00 00 | @J.....J.... |
| Lazy Symbol Pointers | 0053C390 | E0 A9 4A 00 00 00 00 00 | EC A9 4A 00 00 00 00 00 | ..J.....J.... |
| < Section64 __DATA,__mod_init_func) | 0053C3A0 | F8 AB 4A 00 00 00 00 00 | FC AB 4A 00 00 00 00 00 | ..J.....J.... |
| Module Init Func Pointers | 0053C3B0 | 54 AB 4A 00 00 00 00 00 | AC 60 04 00 00 00 00 00 | T.J.....J.... |
| Section64 __DATA,__const) | 0053C3C0 | 60 AB 4A 00 00 00 00 00 | 6C AB 4A 00 00 00 00 00 | ..J.....L.J.... |
| ObjC CFStrings | 0053C3D0 | A8 5E 04 00 00 00 00 00 | 78 AB 4A 00 00 00 00 00 | .^.....x.J.... |
| < Section64 __DATA,__objc_classlist) | 0053C3E0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| ObjC2 Class List | 0053C3F0 | 84 AB 4A 00 00 00 00 00 | 90 AB 4A 00 00 00 00 00 | ..J.....J.... |
| < Section64 __DATA,__objc_catlist) | 0053C400 | 9C AB 4A 00 00 00 00 00 | AB AB 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Category List | 0053C410 | B4 AB 4A 00 00 00 00 00 | C0 AB 4A 00 00 00 00 00 | ..J.....J.... |
| < Section64 __DATA,__objc_imageinfo) | 0053C420 | 08 AC 4A 00 00 00 00 00 | 14 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Image Info | 0053C430 | 20 AC 4A 00 00 00 00 00 | 2C AC 4A 00 00 00 00 00 | .J.....J.... |
| < Section64 __DATA,__objc_const) | 0053C440 | 38 AC 4A 00 00 00 00 00 | 44 AC 4A 00 00 00 00 00 | 8.J....D.J.... |
| ObjC2 Class64 Info: 0x53F5B0 __OBJC_CLASS_R... | 0053C450 | 50 AC 4A 00 00 00 00 00 | 5C AC 4A 00 00 00 00 00 | P.J....\J.... |
| ObjC2 Method64 List: 0x53F5F8 __OBJC_S_CAT... | 0053C460 | 68 AC 4A 00 00 00 00 00 | 74 AC 4A 00 00 00 00 00 | h.J....t.J.... |
| ObjC2 Category64: 0x53F780 __OBJC_S_CATEG... | 0053C470 | 54 AA 4A 00 00 00 00 00 | 64 AA 4A 00 00 00 00 00 | X.J....d.J.... |
| ObjC2 Method64 List: 0x53F808 __OBJC_S_INST... | 0053C480 | 70 AA 4A 00 00 00 00 00 | 80 AC 4A 00 00 00 00 00 | p.J.....J.... |
| ObjC2 Variable64 List: 0x53F7C8 __OBJC_S_INS... | 0053C490 | BC AC 4A 00 00 00 00 00 | 98 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Property64 List: 0x53F400 __OBJC_S_PR... | 0053C4A0 | A4 AC 4A 00 00 00 00 00 | B0 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Class64 Info: 0x5400A8 __OBJC_CLASS_R... | 0053C4B0 | BC AC 4A 00 00 00 00 00 | C8 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Method64 List: 0x540248 __OBJC_S_INST... | 0053C4C0 | D4 AC 4A 00 00 00 00 00 | E0 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Variable64 List: 0x540370 __OBJC_S_INST... | 0053C4D0 | EC AC 4A 00 00 00 00 00 | F8 AC 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Property64 List: 0x540418 __OBJC_S_PR... | 0053C4E0 | 04 AD 4A 00 00 00 00 00 | 10 AD 4A 00 00 00 00 00 | ..J.....J.... |
| ObjC2 Class64 Info: 0x540470 __OBJC_CLASS_R... | 0053C4F0 | 1C AD 4A 00 00 00 00 00 | 28 AD 4A 00 00 00 00 00 | ..J.....(J.... |
| ObjC2 Method64 List: 0x5405050 __OBJC_S_INST... | 0053C500 | 34 AD 4A 00 00 00 00 00 | 40 AD 4A 00 00 00 00 00 | 4.J....@J.... |
| ObjC2 Class64 Info: 0x540570 __OBJC_CLASS_R... | 0053C510 | 4C AD 4A 00 00 00 00 00 | 58 AD 4A 00 00 00 00 00 | L.J....X.J.... |
| < Section64 __DATA,__objc_seirefs) | 0053C520 | 64 AD 4A 00 00 00 00 00 | 70 AD 4A 00 00 00 00 00 | d.J....p.J.... |
| Literal Pointers | 0053C530 | 7C AD 4A 00 00 00 00 00 | 88 AD 4A 00 00 00 00 00 | J.....J.... |
| < Section64 __DATA,__objc_classrefs) | 0053C540 | 7C AA 4A 00 00 00 00 00 | 94 AD 4A 00 00 00 00 00 | J.....J.... |
| | 0053C550 | 88 AD 4A 00 00 00 00 00 | 9E AD 4A 00 00 00 00 00 | 1.J.....J.... |

| zzzzHeiBaoLib.dylib | | | | |
|--|----------|------------------|------------------|--|
| | Offset | Data | Description | Value |
| > Section64 __TEXT,__cstring) | 0053C2F0 | 0000000004AACCC | Indirect Pointer | [0x53C2F0->_CCCrypt] |
| > Section64 __TEXT,__objc_methname) | 0053C2F8 | 0000000004AAAB8 | Indirect Pointer | [0x53C2F8->_CC_MDS_Final] |
| > Section64 __TEXT,__const) | 0053C300 | 0000000004AAE84 | Indirect Pointer | [0x53C300->_CC_MDS_Init] |
| > Section64 __TEXT,__objc_classname) | 0053C308 | 0000000004AAFB8 | Indirect Pointer | [0x53C308->_CC_MDS_Update] |
| > Section64 __TEXT,__objc_methtype) | 0053C310 | 0000000004AAE9C | Indirect Pointer | [0x53C310->_CFDataGetBytePtr] |
| > Section64 __TEXT,__unwind_info) | 0053C318 | 0000000004AAEAE8 | Indirect Pointer | [0x53C318->_CFDataGetLength] |
| > Section64 __TEXT,__eh_frame) | 0053C320 | 0000000004AAEB4 | Indirect Pointer | [0x53C320->_CFDataGetTypeID] |
| > Section64 __DATA,__got) | 0053C328 | 0000000004AAEC0 | Indirect Pointer | [0x53C328->_CFGetTypeID] |
| Non-Lazy Symbol Pointers | 0053C330 | 0000000004AAECC | Indirect Pointer | [0x53C330->_CFNotificationCenterAddObserver] |
| < Section64 __DATA,la_symbol_ptr) | 0053C338 | 0000000004AAE8D | Indirect Pointer | [0x53C338->_CFNotificationCenterGetDarwinNotifyCenter] |
| Lazy Symbol Pointers | 0053C340 | 0000000004AAEED4 | Indirect Pointer | [0x53C340->_CFNotificationCenterPostNotification] |
| < Section64 __DATA,__mod_init_func) | 0053C348 | 0000000004AAE8F0 | Indirect Pointer | [0x53C348->_CFRetain] |
| Module Init Func Pointers | 0053C350 | 0000000004AA9C8 | Indirect Pointer | [0x53C350->_CLLocationCoordinate2DMake] |
| Section64 __DATA,__const) | 0053C358 | 0000000004AA8A04 | Indirect Pointer | [0x53C358->_IORegistryEntryCreateCFProperties] |
| ObjC CFStrings | 0053C360 | 0000000004AA8A10 | Indirect Pointer | [0x53C360->_IORegistryEntryGetName] |
| < Section64 __DATA,__objc_classlist) | 0053C368 | 0000000004AA8A1C | Indirect Pointer | [0x53C368->_MSFindSymbol] |
| ObjC2 Class List | 0053C370 | 0000000004AA8A28 | Indirect Pointer | [0x53C370->_MSGetImageByName] |
| < Section64 __DATA,__objc_catlist) | 0053C378 | 0000000004AA8A34 | Indirect Pointer | [0x53C378->_MSHookFunction] |
| ObjC2 Category List | 0053C380 | 0000000004AA8A40 | Indirect Pointer | [0x53C380->_MSHookMessageEx] |
| < Section64 __DATA,__objc_imageinfo) | 0053C388 | 0000000004AA9D94 | Indirect Pointer | [0x53C388->_NSClassFromString] |
| ObjC2 Image Info | 0053C390 | 0000000004AA9E0 | Indirect Pointer | [0x53C390->_NSHomeDirectory] |
| < Section64 __DATA,__objc_const) | 0053C398 | 0000000004AA9E9C | Indirect Pointer | [0x53C398->_NSSearchPathForDirectoriesInDomains] |
| ObjC2 Class64 Info: 0x53F5B0 __OBJC_CLASS_R... | 0053C3A0 | 0000000004AA9F8 | Indirect Pointer | [0x53C3A0->_NSSetUncaughtExceptionHandler] |
| ObjC2 Method64 List: 0x53F5F8 __OBJC_S_CAT... | 0053C3A8 | 0000000004AAFB8 | Indirect Pointer | [0x53C3A8->_Unwind_Resume] |
| ObjC2 Category64: 0x53F780 __OBJC_S_CATEG... | 0053C3B0 | 0000000004AA854 | Indirect Pointer | [0x53C3B0->_ZNKSt12__vector_base_commonIlb1EE20_throw_length_error_ |
| ObjC2 Method64 List: 0x53F808 __OBJC_S_INST... | 0053C3B8 | 0000000004A60AC | Indirect Pointer | [0x53C3B8->_ZNKSt16vectorI14_RuntimeModuleNS_9allocatorIS1_EEE8max_ |
| ObjC2 Variable64 List: 0x53F7C8 __OBJC_S_INS... | 0053C3C0 | 0000000004AA8B0 | Indirect Pointer | [0x53C3C0->_ZNSt11logic_errorZC2PKc] |
| ObjC2 Property64 List: 0x53F400 __OBJC_S_PR... | 0053C3C8 | 0000000004AA8B6C | Indirect Pointer | [0x53C3C8->_ZNSt8__basic_stringI NS_1char_traitsIcEENS_9allocatorIS1_EEE26_sw_ |
| ObjC2 Class64 Info: 0x5400A8 __OBJC_CLASS_R... | 0053C3D0 | 0000000004AAE8 | Indirect Pointer | [0x53C3D0->_ZNSt16vectorI14_RuntimeModuleNS_9allocatorIS1_EEE26_sw_ |
| ObjC2 Method64 List: 0x540248 __OBJC_S_INST... | 0053C3D8 | 0000000004AA878 | Indirect Pointer | [0x53C3D8->_ZSI9terminatev] |
| ObjC2 Variable64 List: 0x540370 __OBJC_S_INST... | 0053C3E0 | 0000000004AA8000 | Indirect Pointer | [0x53C3E0->_ZdPv] |
| ObjC2 Property64 List: 0x540418 __OBJC_S_PR... | 0053C3E8 | 0000000004AA8B4 | Indirect Pointer | [0x53C3E8->_Znwm] |
| ObjC2 Class64 Info: 0x540470 __OBJC_CLASS_R... | 0053C3F0 | 0000000004AA8B84 | Indirect Pointer | [0x53C3F0->_cxa_allocate_exception] |
| ObjC2 Method64 List: 0x5405050 __OBJC_S_INST... | 0053C3F8 | 0000000004AA8B90 | Indirect Pointer | [0x53C3F8->_cxa_begin_catch] |
| ObjC2 Class64 Info: 0x540570 __OBJC_CLASS_R... | 0053C400 | 0000000004AA89C | Indirect Pointer | [0x53C400->_cxa_free_exception] |
| < Section64 __DATA,__objc_seirefs) | 0053C408 | 0000000004AA8A8B | Indirect Pointer | [0x53C408->_cxa_guard_acquire] |
| Literal Pointers | 0053C410 | 0000000004AA8B4 | Indirect Pointer | [0x53C410->_cxa_guard_release] |
| < Section64 __DATA,__objc_classrefs) | 0053C418 | 0000000004AA8C0 | Indirect Pointer | [0x53C418->_cxa_throw] |
| | 0053C420 | 0000000004AA8A8A | Indirect Pointer | [0x53C420->_error] |

| zzzzHeiBaoLib.dylib | | | | |
|---|--------|------|------------------|---|
| | Offset | Data | Description | Value |
| > Section64 __TEXT,__cstring | | | | |
| > Section64 __TEXT,__objc_methname | | | Indirect Pointer | [0x53C550->_mprotect] |
| Section64 __TEXT,__const | | | Indirect Pointer | [0x53C558->_munmap] |
| > Section64 __TEXT,__objc_classname | | | Indirect Pointer | [0x53C560->_objc_alloc] |
| > Section64 __TEXT,__objc_methtype | | | Indirect Pointer | [0x53C568->_objc_autorelease] |
| Section64 __TEXT,__ustring | | | Indirect Pointer | [0x53C570->_objc_autoreleaseReturnValue] |
| Section64 __TEXT,__ unwind_info | | | Indirect Pointer | [0x53C578->_objc_enumerationMutation] |
| > Section64 __TEXT,__eh_frame | | | Indirect Pointer | [0x53C580->_objc_getAssociatedObject] |
| > Section64 __DATA,__got | | | Indirect Pointer | [0x53C588->_objc_getClassList] |
| Non-Lazy Symbol Pointers | | | Indirect Pointer | [0x53C590->_objc_release] |
| > Section64 __DATA,__la_symbol_ptr | | | Indirect Pointer | [0x53C598->_objc_retain] |
| Lazy Symbol Pointers | | | Indirect Pointer | [0x53C5A0->_objc_retainAutorelease] |
| > Section64 __DATA,__mod_init_func | | | Indirect Pointer | [0x53C5A8->_objc_retainAutoreleaseReturnValue] |
| Module Init Func Pointers | | | Indirect Pointer | [0x53C5B0->_objc_retainAutoreleasedReturnValue] |
| Section64 __DATA,__const | | | Indirect Pointer | [0x53C5B8->_objc_retainBlock] |
| > Section64 __DATA,__cfstring | | | Indirect Pointer | [0x53C5C0->_objc_setAssociatedObject] |
| ObjC CFStrings | | | Indirect Pointer | [0x53C5C8->_objc_storeStrong] |
| > Section64 __DATA,__objc_classlist | | | Indirect Pointer | [0x53C5D0->_objc_unsafeClaimAutoreleasedReturnValue] |
| ObjC2 Class List | | | Indirect Pointer | [0x53C5D8->_object_getClass] |
| > Section64 __DATA,__objc_catlist | | | Indirect Pointer | [0x53C5E0->_property_getName] |
| ObjC2 Category List | | | Indirect Pointer | [0x53C5E8->_rocketbootstrap_distributedMessagingcenter_apply] |
| > Section64 __DATA,__objc_imageinfo | | | Indirect Pointer | [0x53C5F0->_sleep] |
| ObjC2 Image Info | | | Indirect Pointer | [0x53C5F8->_strcmp] |
| > Section64 __DATA,__objc_const | | | Indirect Pointer | [0x53C600->_strdup] |
| ObjC2 Class64 Info: 0x53F5B0 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C608->_strlcpy] |
| ObjC2 Method64 List: 0x53F5F8 __OBJC_S_CAT... | | | Indirect Pointer | [0x53C610->_strlen] |
| ObjC2 Category64: 0x53F780 __OBJC_S_CATEG... | | | Indirect Pointer | [0x53C618->_strncmp] |
| ObjC2 Method64 List: 0x53F808 __OBJC_S_INST... | | | Indirect Pointer | [0x53C620->_strncpy] |
| ObjC2 Variable64 List: 0x53FC78 __OBJC_S_INS... | | | Indirect Pointer | [0x53C628->_strstr] |
| ObjC2 Property64 List: 0x53FF40 __OBJC_S_PR... | | | Indirect Pointer | [0x53C630->_strtol] |
| ObjC2 Class64 Info: 0x5400A8 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C638->_sys_icache_invalidate] |
| ObjC2 Method64 List: 0x540248 __OBJC_S_INST... | | | Indirect Pointer | [0x53C640->_sysconf] |
| ObjC2 Variable64 List: 0x540370 __OBJC_S_INS... | | | Indirect Pointer | [0x53C648->_task_info] |
| ObjC2 Property64 List: 0x540418 __OBJC_S_PR... | | | Indirect Pointer | [0x53C650->_time] |
| ObjC2 Class64 Info: 0x540470 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C658->_vm_protect] |
| ObjC2 Method64 List: 0x540550 __OBJC_S_INST... | | | Indirect Pointer | [0x53C660->_vm_region_64] |
| ObjC2 Class64 Info: 0x540570 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C668->_vm_write] |
| > Section64 __DATA,__objc_selrefs | | | Indirect Pointer | [0x53C670->_vprintf] |
| Literal Pointers | | | Indirect Pointer | [0x53C678->_vsprintf] |
| > Section64 __DATA,__objc_classrefs | | | Indirect Pointer | [0x53C680->_vsyslog] |

分析：

其中很多函数，就是IDA中Imports的函数：

| zzzzHeiBaoLib.dylib | | | | |
|---|--------|------|------------------|---|
| | Offset | Data | Description | Value |
| > Section64 __TEXT,__cstring | | | | |
| > Section64 __TEXT,__objc_methname | | | Indirect Pointer | [0x53C400->_cxa_free_exception] |
| Section64 __TEXT,__const | | | Indirect Pointer | [0x53C408->_cxa_guard_acquire] |
| > Section64 __TEXT,__objc_classname | | | Indirect Pointer | [0x53C410->_cxa_guard_release] |
| > Section64 __TEXT,__objc_methtype | | | Indirect Pointer | [0x53C418->_cxa_throw] |
| Section64 __TEXT,__ustring | | | Indirect Pointer | [0x53C420->_error] |
| Section64 __TEXT,__ unwind_info | | | Indirect Pointer | [0x53C428->_memcpy_chk] |
| > Section64 __TEXT,__eh_frame | | | Indirect Pointer | [0x53C430->_stack_chk_fail] |
| > Section64 __DATA,__got | | | Indirect Pointer | [0x53C438->_dyld_get_image_header] |
| Non-Lazy Symbol Pointers | | | Indirect Pointer | [0x53C440->_dyld_get_image_name] |
| > Section64 __DATA,__la_symbol_ptr | | | Indirect Pointer | [0x53C448->_dyld_get_image_vmaddr_slide] |
| Lazy Symbol Pointers | | | Indirect Pointer | [0x53C450->_dyld_image_count] |
| > Section64 __DATA,__mod_init_func | | | Indirect Pointer | [0x53C458->_dyld_register_func_for_add_image] |
| Module Init Func Pointers | | | Indirect Pointer | [0x53C460->_dyld_random] |
| Section64 __DATA,__const | | | Indirect Pointer | [0x53C468->_bzero] |
| > Section64 __DATA,__cfstring | | | Indirect Pointer | [0x53C470->_class_copyPropertyList] |
| ObjC CFStrings | | | Indirect Pointer | [0x53C478->_class_getInstanceMethod] |
| > Section64 __DATA,__objc_classlist | | | Indirect Pointer | [0x53C480->_class_getMethodImplementation] |
| ObjC2 Class List | | | Indirect Pointer | [0x53C488->_dispatch_after] |
| > Section64 __DATA,__objc_catlist | | | Indirect Pointer | [0x53C490->_dispatch_async] |
| ObjC2 Category List | | | Indirect Pointer | [0x53C498->_dispatch_once] |
| > Section64 __DATA,__objc_imageinfo | | | Indirect Pointer | [0x53C4A0->_dispatch_time] |
| ObjC2 Image Info | | | Indirect Pointer | [0x53C4A8->_dlaaddr] |
| > Section64 __DATA,__objc_const | | | Indirect Pointer | [0x53C4AB->_dladdr] |
| ObjC2 Class64 Info: 0x53F5B0 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C4B0->_dlopen] |
| ObjC2 Method64 List: 0x53F5F8 __OBJC_S_CAT... | | | Indirect Pointer | [0x53C4B8->_dlsym] |
| ObjC2 Category64: 0x53F780 __OBJC_S_CATEG... | | | Indirect Pointer | [0x53C4C0->_fclose] |
| ObjC2 Method64 List: 0x53F808 __OBJC_S_INST... | | | Indirect Pointer | [0x53C4C8->_fcntl] |
| ObjC2 Variable64 List: 0x53FC78 __OBJC_S_INS... | | | Indirect Pointer | [0x53C4D0->_fflush] |
| ObjC2 Property64 List: 0x53FF40 __OBJC_S_PR... | | | Indirect Pointer | [0x53C4D8->_fopen] |
| ObjC2 Class64 Info: 0x5400A8 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C4E0->_free] |
| ObjC2 Method64 List: 0x540248 __OBJC_S_INST... | | | Indirect Pointer | [0x53C4E8->_fopen] |
| ObjC2 Variable64 List: 0x540370 __OBJC_S_INS... | | | Indirect Pointer | [0x53C4F0->_fwrite] |
| ObjC2 Property64 List: 0x540418 __OBJC_S_PR... | | | Indirect Pointer | [0x53C4F8->_getsectbynamefromheader_64] |
| ObjC2 Class64 Info: 0x540470 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C500->_inet_ntoa] |
| ObjC2 Method64 List: 0x540550 __OBJC_S_INST... | | | Indirect Pointer | [0x53C508->_inet_pton] |
| ObjC2 Class64 Info: 0x540570 __OBJC_CLASS_R... | | | Indirect Pointer | [0x53C510->_lstat] |
| > Section64 __DATA,__objc_selrefs | | | Indirect Pointer | [0x53C518->_mach_vm_remap] |
| Literal Pointers | | | Indirect Pointer | [0x53C520->_malloc] |
| > Section64 __DATA,__objc_classrefs | | | Indirect Pointer | [0x53C528->_memcmp] |

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 23:17:45

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

| Address | Data | Description | Value |
|---------------------------------------|------------------|------------------|---------------------------------------|
| 100002000 | 0000000000000000 | Indirect Pointer | [0x100002000->__stack_chk_guard] |
| 100002008 | 0000000000000000 | Indirect Pointer | [0x100002008->_kCFAllocatorDefault] |
| 100002010 | 0000000000000000 | Indirect Pointer | [0x100002010->_kCFRunLoopDefaultMode] |
| 100002018 | 0000000000000000 | Indirect Pointer | [0x100002018->_mach_task_self_] |
| 100002020 | 0000000000000000 | Indirect Pointer | [0x100002020->dyld_stub_binder] |
| Non-Lazy Symbol Pointers | | | |
| Section64 __DATA_CONST__const | | | |
| Section64 __DATA_CONST__la_symbol_ptr | | | |

@稀土掘金技术社区

- zzzzHeiBaoLib.dylib

Shared Library (ARM64_ALL)

| Offset | Data | Description | Value |
|-----------|------------------|------------------|---|
| 0x053C000 | 0000000000000000 | Indirect Pointer | [0x53C000->_CGRectZero] |
| 0x053C008 | 0000000000000000 | Indirect Pointer | [0x53C008->_NCopyCurrentNetworkInfo] |
| 0x053C010 | 0000000000000000 | Indirect Pointer | [0x53C010->_CTRadioAccessTechnologyLTE] |
| 0x053C018 | 0000000000000000 | Indirect Pointer | [0x53C018->_IORRegistryEntryCreateCFProperties] |
| 0x053C020 | 0000000000000000 | Indirect Pointer | [0x53C020->_IORRegistryEntrySearchCFProperty] |
| 0x053C028 | 0000000000000000 | Indirect Pointer | [0x53C028->_IORRegistryEntrySearchCFProperty] |
| 0x053C030 | 0000000000000000 | Indirect Pointer | [0x53C030->_NSCocoaErrorDomain] |
| 0x053C038 | 0000000000000000 | Indirect Pointer | [0x53C038->_NSFileCreationDate] |
| 0x053C040 | 0000000000000000 | Indirect Pointer | [0x53C040->_NSFileModificationDate] |
| 0x053C048 | 0000000000000000 | Indirect Pointer | [0x53C048->_NSFileSystemFreeSize] |
| 0x053C050 | 0000000000000000 | Indirect Pointer | [0x53C050->_NSFoundationVersionNumber] |
| 0x053C058 | 0000000000000000 | Indirect Pointer | [0x53C058->_NSInternalInconsistencyException] |
| 0x053C060 | 0000000000000000 | Indirect Pointer | [0x53C060->_NSPOSIXErrorDomain] |
| 0x053C068 | 0000000000000000 | Indirect Pointer | [0x53C068->_NSPOSIXErrorDomain] |
| 0x053C070 | 0000000000000000 | Indirect Pointer | [0x53C070->_NSRunLoopCommonModes] |
| 0x053C078 | 0000000000000000 | Indirect Pointer | [0x53C078->_SNetworkReachabilityGetFlags] |
| 0x053C080 | 0000000000000000 | Indirect Pointer | [0x53C080->_UIApplicationMain] |
| 0x053C088 | 0000000000000000 | Indirect Pointer | [0x53C088->_NSConcreteGlobalBlock] |
| 0x053C090 | 0000000000000000 | Indirect Pointer | [0x53C090->_NSConcreteStackBlock] |
| 0x053C098 | 0000000000000000 | Indirect Pointer | [0x53C098->_ZNSt12length_error@E] |
| 0x053C0A0 | 0000000000000000 | Indirect Pointer | [0x53C0A0->_ZTVSt12length_error] |
| 0x053C0A8 | 0000000000000000 | Indirect Pointer | [0x53C0A8->_NSDictionary@_] |
| 0x053C0B0 | 0000000000000000 | Indirect Pointer | [0x53C0B0->_qx_personality@_v0] |
| 0x053C0B8 | 0000000000000000 | Indirect Pointer | [0x53C0B8->_openDir2] |
| 0x053C0C0 | 0000000000000000 | Indirect Pointer | [0x53C0C0->_stack_chk_guard] |
| 0x053C0C8 | 0000000000000000 | Indirect Pointer | [0x53C0C8->_stderpp] |
| 0x053C0D0 | 0000000000000000 | Indirect Pointer | [0x53C0D0->_stdoutp] |
| 0x053C0D8 | 0000000000000000 | Indirect Pointer | [0x53C0D8->_dispatch_main_q] |
| 0x053C0E0 | 0000000000000000 | Indirect Pointer | [0x53C0E0->_dyld_get_image_header] |
| 0x053C0E8 | 0000000000000000 | Indirect Pointer | [0x53C0E8->_dyld_get_image_name] |
| 0x053C0F0 | 0000000000000000 | Indirect Pointer | [0x53C0F0->_dyld_get_image_vmaaddr_slide] |
| 0x053C0F8 | 0000000000000000 | Indirect Pointer | [0x53C0F8->_dyld_image_count] |
| 0x053C100 | 0000000000000000 | Indirect Pointer | [0x53C100->_access] |
| 0x053C108 | 0000000000000000 | Indirect Pointer | [0x53C108->_chdir] |
| 0x053C110 | 0000000000000000 | Indirect Pointer | [0x53C110->_chroot] |
| 0x053C118 | 0000000000000000 | Indirect Pointer | [0x53C118->_connect] |
| 0x053C120 | 0000000000000000 | Indirect Pointer | [0x53C120->_create] |
| 0x053C128 | 0000000000000000 | Indirect Pointer | [0x53C128->_dlaaddr] |
| 0x053C130 | 0000000000000000 | Indirect Pointer | [0x53C130->_dlopen_rnflint] |

Shared Library (ARM64_ALL)

| Offset | Data | Description | Value |
|-----------|------------------|------------------|---|
| 0x053C1B8 | 0000000000000000 | Indirect Pointer | [0x53C1B8->_getxattr] |
| 0x053C1C0 | 0000000000000000 | Indirect Pointer | [0x53C1C0->_loctl] |
| 0x053C1C8 | 0000000000000000 | Indirect Pointer | [0x53C1C8->_kCFAllocatorDefault] |
| 0x053C1D0 | 0000000000000000 | Indirect Pointer | [0x53C1D0->_kCFCoreFoundationVersionNumber] |
| 0x053C1D8 | 0000000000000000 | Indirect Pointer | [0x53C1D8->_link] |
| 0x053C1E0 | 0000000000000000 | Indirect Pointer | [0x53C1E0->_listxattr] |
| 0x053C1E8 | 0000000000000000 | Indirect Pointer | [0x53C1E8->_lstat] |
| 0x053C1F0 | 0000000000000000 | Indirect Pointer | [0x53C1F0->_mach_task_self_] |
| 0x053C1F8 | 0000000000000000 | Indirect Pointer | [0x53C1F8->_objc_copyClassNamesForImage] |
| 0x053C200 | 0000000000000000 | Indirect Pointer | [0x53C200->_objc_copyImageNames] |
| 0x053C208 | 0000000000000000 | Indirect Pointer | [0x53C208->_open] |
| 0x053C210 | 0000000000000000 | Indirect Pointer | [0x53C210->_openat] |
| 0x053C218 | 0000000000000000 | Indirect Pointer | [0x53C218->_popen] |
| 0x053C220 | 0000000000000000 | Indirect Pointer | [0x53C220->_posix_spawn] |
| 0x053C228 | 0000000000000000 | Indirect Pointer | [0x53C228->_posix_spawnp] |
| 0x053C230 | 0000000000000000 | Indirect Pointer | [0x53C230->_readlink] |
| 0x053C232 | 0000000000000000 | Indirect Pointer | [0x53C232->_realpath\$Darwin_ExtSN] |
| 0x053C240 | 0000000000000000 | Indirect Pointer | [0x53C240->_remove] |
| 0x053C248 | 0000000000000000 | Indirect Pointer | [0x53C248->_rename] |
| 0x053C250 | 0000000000000000 | Indirect Pointer | [0x53C250->_mdir] |
| 0x053C258 | 0000000000000000 | Indirect Pointer | [0x53C258->_scandir] |
| 0x053C260 | 0000000000000000 | Indirect Pointer | [0x53C260->_Setegid] |
| 0x053C268 | 0000000000000000 | Indirect Pointer | [0x53C268->_seteuid] |
| 0x053C270 | 0000000000000000 | Indirect Pointer | [0x53C270->_setgid] |
| 0x053C278 | 0000000000000000 | Indirect Pointer | [0x53C278->_setregid] |
| 0x053C280 | 0000000000000000 | Indirect Pointer | [0x53C280->_setregid] |
| 0x053C288 | 0000000000000000 | Indirect Pointer | [0x53C288->_setuid] |
| 0x053C290 | 0000000000000000 | Indirect Pointer | [0x53C290->_stat] |
| 0x053C298 | 0000000000000000 | Indirect Pointer | [0x53C298->_stafs] |
| 0x053C2A0 | 0000000000000000 | Indirect Pointer | [0x53C2A0->_symlink] |
| 0x053C2A8 | 0000000000000000 | Indirect Pointer | [0x53C2A8->_syscall1] |
| 0x053C2B0 | 0000000000000000 | Indirect Pointer | [0x53C2B0->_sysctl] |
| 0x053C2B8 | 0000000000000000 | Indirect Pointer | [0x53C2B8->_sysctlbyname] |
| 0x053C2C0 | 0000000000000000 | Indirect Pointer | [0x53C2C0->_task_info] |
| 0x053C2C8 | 0000000000000000 | Indirect Pointer | [0x53C2C8->_uname] |
| 0x053C2D0 | 0000000000000000 | Indirect Pointer | [0x53C2D0->_unlink] |
| 0x053C2D8 | 0000000000000000 | Indirect Pointer | [0x53C2D8->_unlinkat] |
| 0x053C2E0 | 0000000000000000 | Indirect Pointer | [0x53C2E0->_fork] |
| 0x053C2E8 | 0000000000000000 | Indirect Pointer | [0x53C2E8->_dyld_stub_binder] |

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 23:17:18

__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.

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:

2023-10-06 16:28:34

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 17:16:38

__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。

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 17:15:43

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 */
}

```

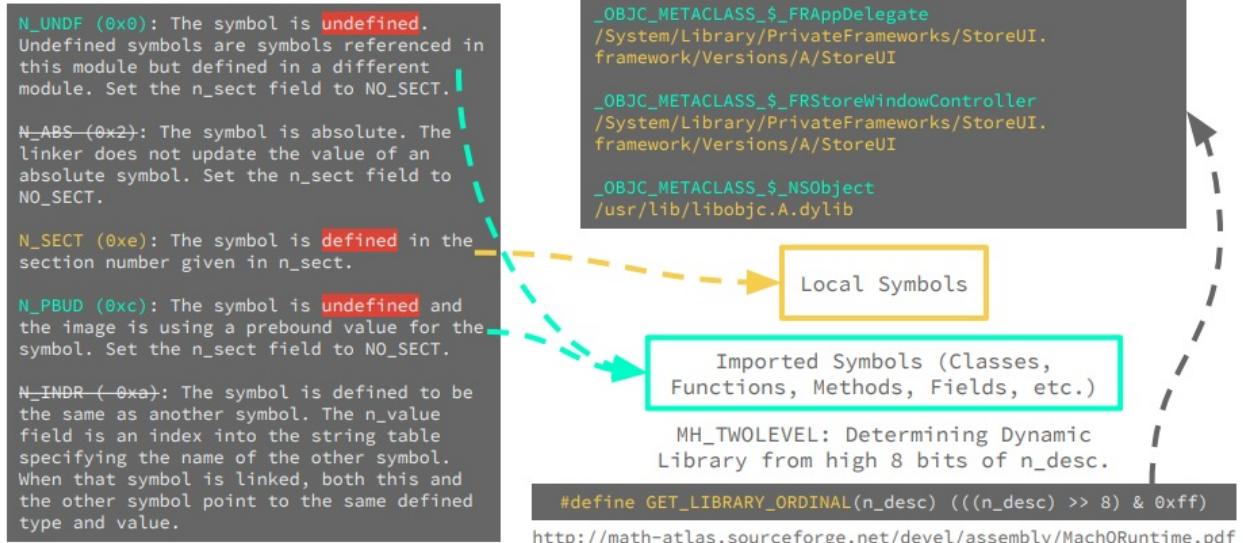
```
    uint32_t offset;      /* file offset of this section */
    uint32_t align;       /* section alignment (power of 2) */
    uint32_t reloff;     /* file offset of relocation entries */
    uint32_t nreloc;     /* number of relocation entries */
    uint32_t flags;       /* flags (section type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


```

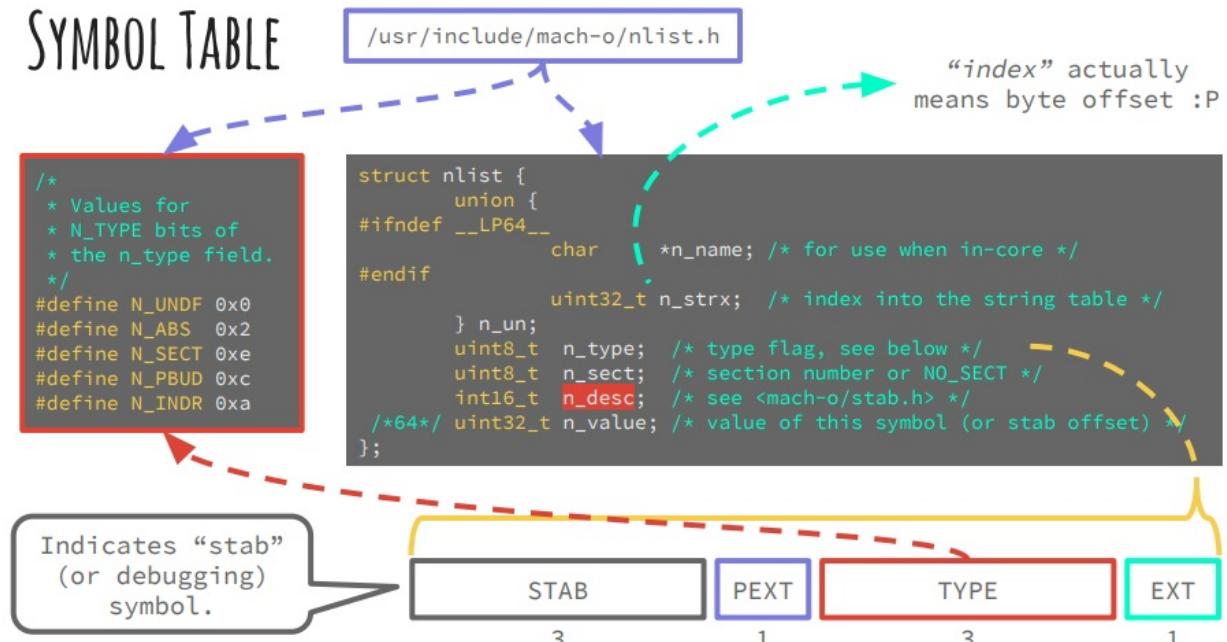
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-06 16:28:56

symbol

SYMBOLS... BUT WHAT DO THEY MEAN?!



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 [GMRYouHaoHuReq getRequestURL]
- 地址是 0x100003300

string

- String Table
 - String表顺序列出了二进制mach-O文件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]

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-06 17:27:05

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-05 16:43:09

FAT举例

用MachOView查看

RevealServer

| Offset | Data | Description | Value |
|----------|----------|------------------------|------------------------|
| 00000000 | BEBAFECA | Magic Number | FAT_CIGAM |
| 00000004 | 05000000 | Number of Architecture | 5 |
| 00000008 | 07000000 | CPU Type | CPU_TYPE_I386 |
| 0000000C | 03000000 | CPU SubType | CPU_SUBTYPE_I386_ALL |
| 00000010 | 00100000 | Offset | 4096 |
| 00000014 | 20571000 | Size | 1070880 |
| 00000018 | 0C000000 | Align | 4096 |
| 0000001C | 07000001 | CPU Type | CPU_TYPE_X86_64 |
| 00000020 | 03000000 | CPU SubType | CPU_SUBTYPE_X86_64_ALL |
| 00000024 | 00701000 | Offset | 1077248 |
| 00000028 | 90101200 | Size | 1183888 |
| 0000002C | 0C000000 | Align | 4096 |
| 00000030 | 0C000000 | CPU Type | CPU_TYPE_ARM |
| 00000034 | 09000000 | CPU SubType | CPU_SUBTYPE_ARM_V7 |
| 00000038 | 00C02200 | Offset | 2277376 |
| 0000003C | D0854400 | Size | 4490704 |
| 00000040 | 0E000000 | Align | 16384 |
| 00000044 | 0C000001 | CPU Type | CPU_TYPE_ARM64 |
| 00000048 | 00000000 | CPU SubType | CPU_SUBTYPE_ARM64_ALL |
| 0000004C | 00806700 | Offset | 6782976 |
| 00000050 | D03A4700 | Size | 4668112 |
| 00000054 | 0E000000 | Align | 16384 |
| 00000058 | 0C000001 | CPU Type | CPU_TYPE_ARM64 |
| 0000005C | 02000000 | CPU SubType | ??? |
| 00000060 | 00C0AE00 | Offset | 11452416 |
| 00000064 | 90041200 | Size | 1180816 |
| 00000068 | 0E000000 | Align | 16384 |

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

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 executable 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 executable 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/Developer/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/Developer/usr/bin" file debugserver
debugserver: Mach-O universal binary with 2 architectures: [arm64:Mach-O 64-bit executable 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
```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 17:54:17

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 :

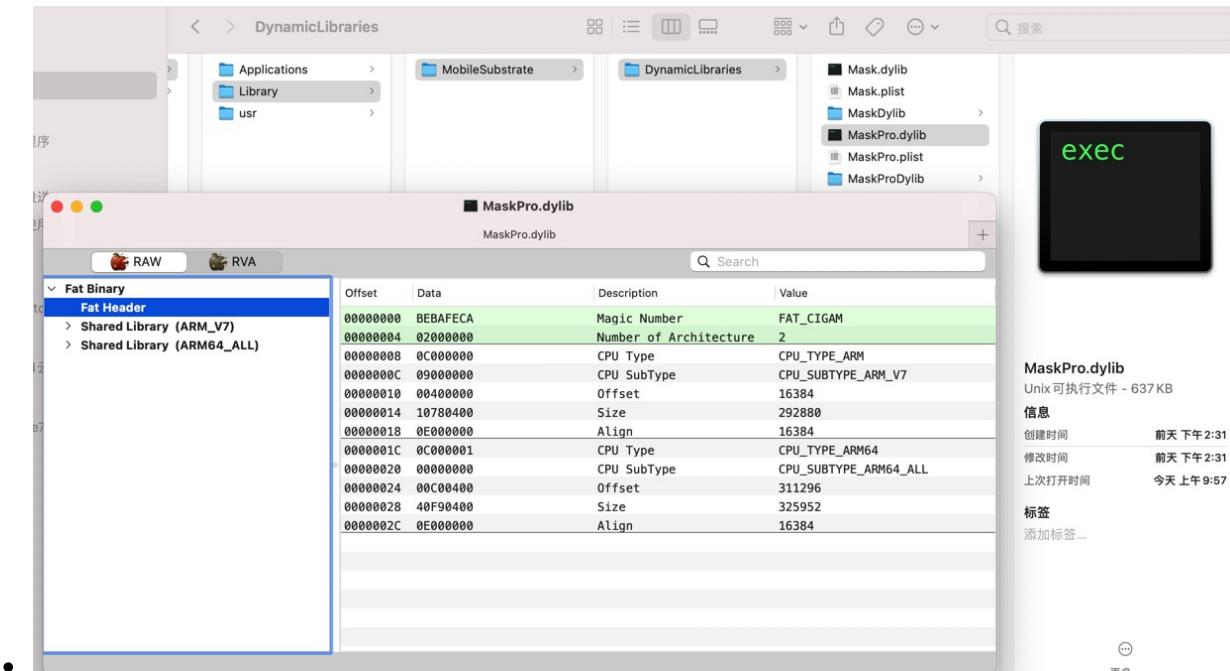
```
→ DynamicLibraries jtool2 -h MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_h_header.txt
Fat binary, little-endian, 2 architectures: armv7, arm64
Select an architecture setting the ARCH= environment variable
```

即，一个Dylib中，包含了多种架构，此处是 armv7 和 arm64

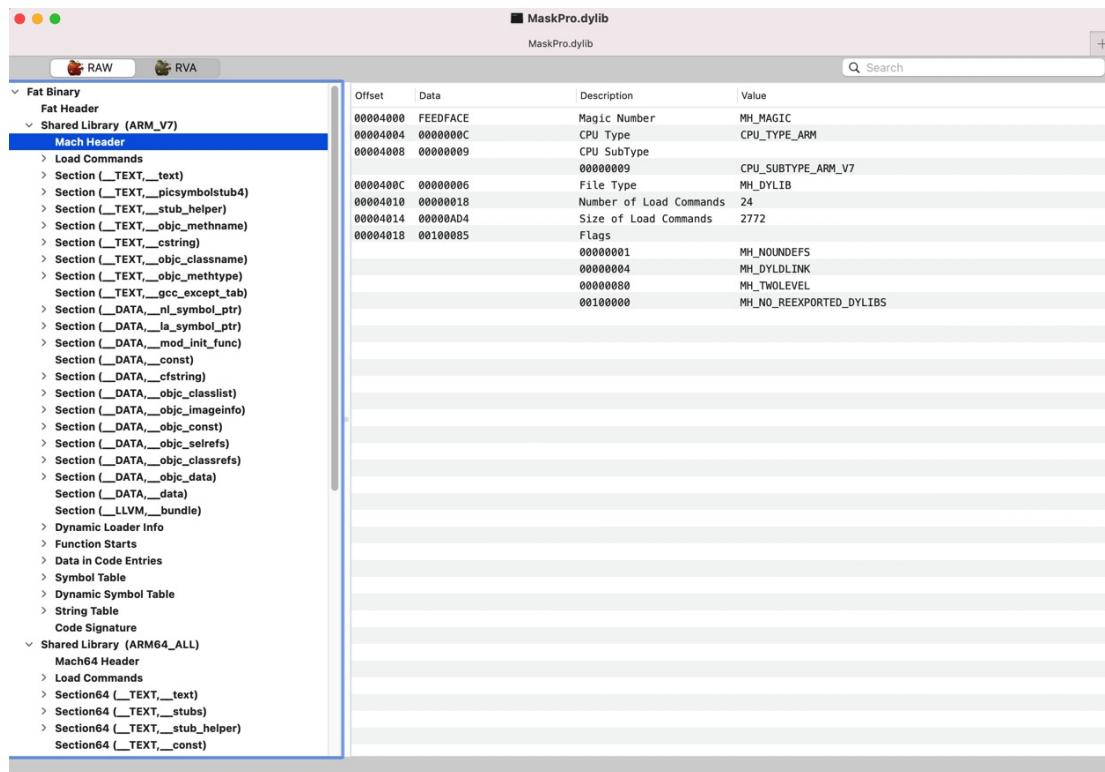
此处要指定具体架构，才能继续用 jtool2 查看信息：

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

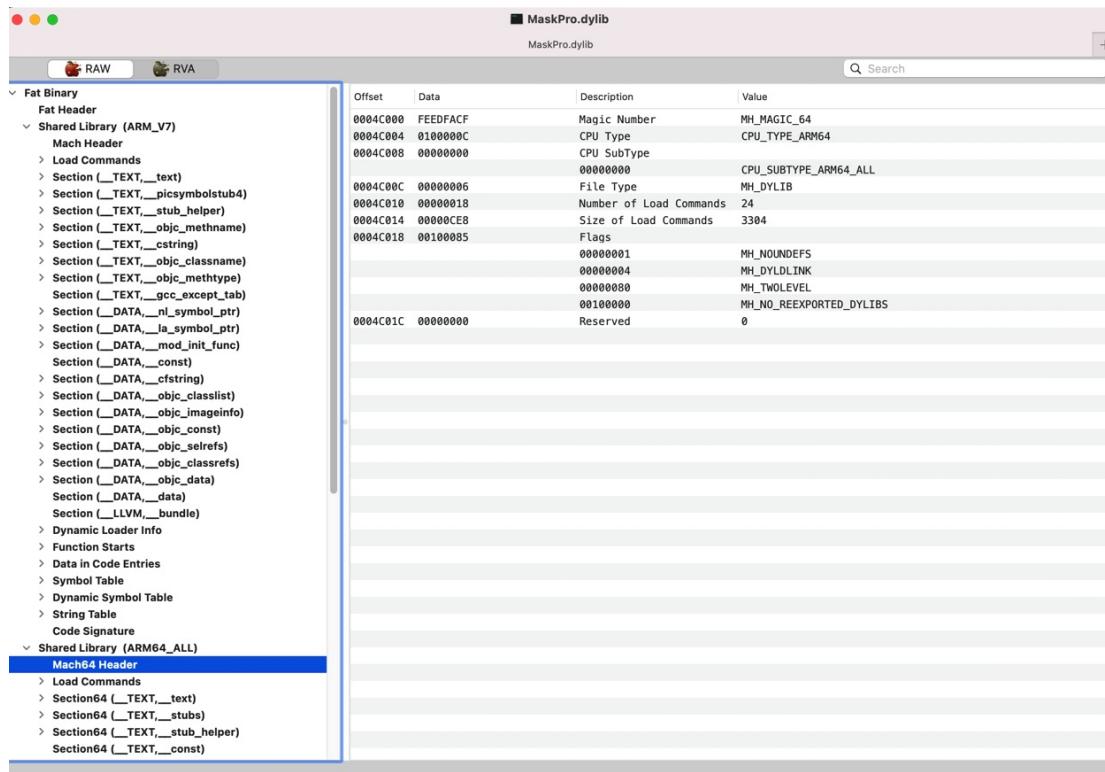
类似的，后续去用 MachOView 查看信息，也能看到是：FAT Binary



- ARMV7



- ARM64



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-05 16:43:30

FAT工具

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-05 16:43:41

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 inputMacOFile -thin ArchType -output OutputFile
```

- 合并多种架构

```
lipo inputMacOFile1 inputMacOFile2 -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



<https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/RequirementLang/RequirementLang.html>

CODE SIGNATURES: BLOBS ON BLOBS ON BLOBS...

```
/*
 * 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 */
};
```

opensource.apple.com

[libsecurity_utilities/lib/blob.h](https://opensource.apple.com)

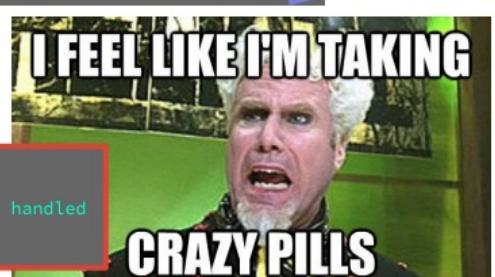
```
///
/// A generic blob wrapped around arbitrary (flat) binary data.
/// This can be used to "regularize" plain binary data, so it can be handled
/// as a genuine Blob (e.g. for insertion into a SuperBlob).
///
```



BLOB?

BLOBWRAPPER???

SUPERBLOB!!!



BLOBS: THEY'RE NOT SO BAD...

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

Specific to Blob type

Standard for every Blob

```
/*
 * 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;
```

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-05 23:13:30

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 = 虚拟内存地址
 - 址 : 0x100000000
 - File Offset 地址: 0xA0460 -> 变成了 RVA 地址: 0x1000A0460

■ 举例

■ akd

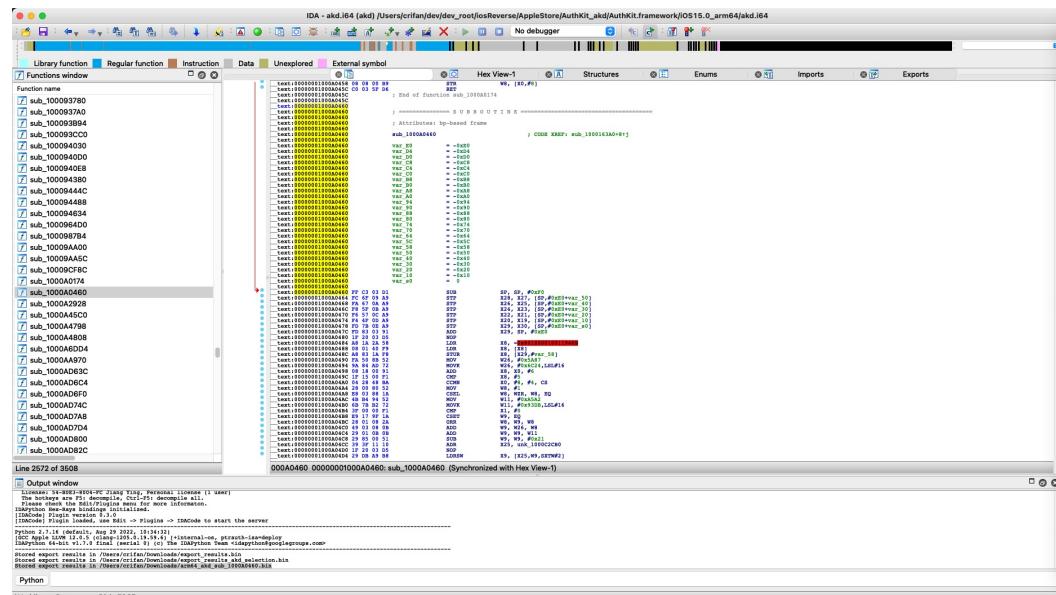
■ RAW

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|--------------------------|
| 00000000 | 5F5F7465787400000000000000000000 | Section Name | __text |
| 0000000C | 5F5F7455540000000000000000000000 | Segment Name | __TEXT |
| 0000000B | 00000000000000000000000000000000 | Address | 4294964656 |
| 00000000 | 00000000000000000000000000000000 | Size | 752468 |
| 00000000 | 00000000000000000000000000000000 | Offset | 17368 |
| 00000004 | 00000000000000000000000000000000 | Alignment | 4 |
| 00000008 | 00000000000000000000000000000000 | Relocations Offset | 0 |
| 0000000C | 00000000000000000000000000000000 | Number of Relocations | 0 |
| 0000000F | 00000000000000000000000000000000 | Flags | 00000000 |
| 00000000 | 00000000000000000000000000000000 | | S_REGULAR |
| 00000000 | 00000000000000000000000000000000 | | S_ATTR_PURE_INSTRUCTIONS |
| 00000004 | 00000000000000000000000000000000 | Reserved1 | 0 |
| 00000008 | 00000000000000000000000000000000 | Reserved2 | 0 |
| 0000000C | 00000000000000000000000000000000 | Reserved3 | 0 |

■ RVA

| Address | Data | Description | Value |
|----------|----------------------------------|-----------------------|--------------------------|
| 10000000 | 5F5F7465787400000000000000000000 | Section Name | __text |
| 1000000C | 5F5F7455540000000000000000000000 | Segment Name | __TEXT |
| 1000000B | 00000000000000000000000000000000 | Address | 4294964656 |
| 10000000 | 00000000000000000000000000000000 | Size | 752468 |
| 10000000 | 00000000000000000000000000000000 | Offset | 17368 |
| 10000004 | 00000000000000000000000000000000 | Alignment | 4 |
| 10000008 | 00000000000000000000000000000000 | Relocations Offset | 0 |
| 1000000C | 00000000000000000000000000000000 | Number of Relocations | 0 |
| 1000000F | 00000000000000000000000000000000 | Flags | 00000000 |
| 10000000 | 00000000000000000000000000000000 | | S_REGULAR |
| 10000000 | 00000000000000000000000000000000 | | S_ATTR_PURE_INSTRUCTIONS |
| 10000004 | 00000000000000000000000000000000 | Reserved1 | 0 |
| 10000008 | 00000000000000000000000000000000 | Reserved2 | 0 |
| 1000000C | 00000000000000000000000000000000 | Reserved3 | 0 |

- IDA中的地址是: 加了基地址后的 RVA 地址



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 22:03:18

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 Executable Size. The size of your app's executable 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**

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：

2023-10-07 22:16:47

Mach-O工具

此处整理查看解析Mach-O文件信息的常用工具。

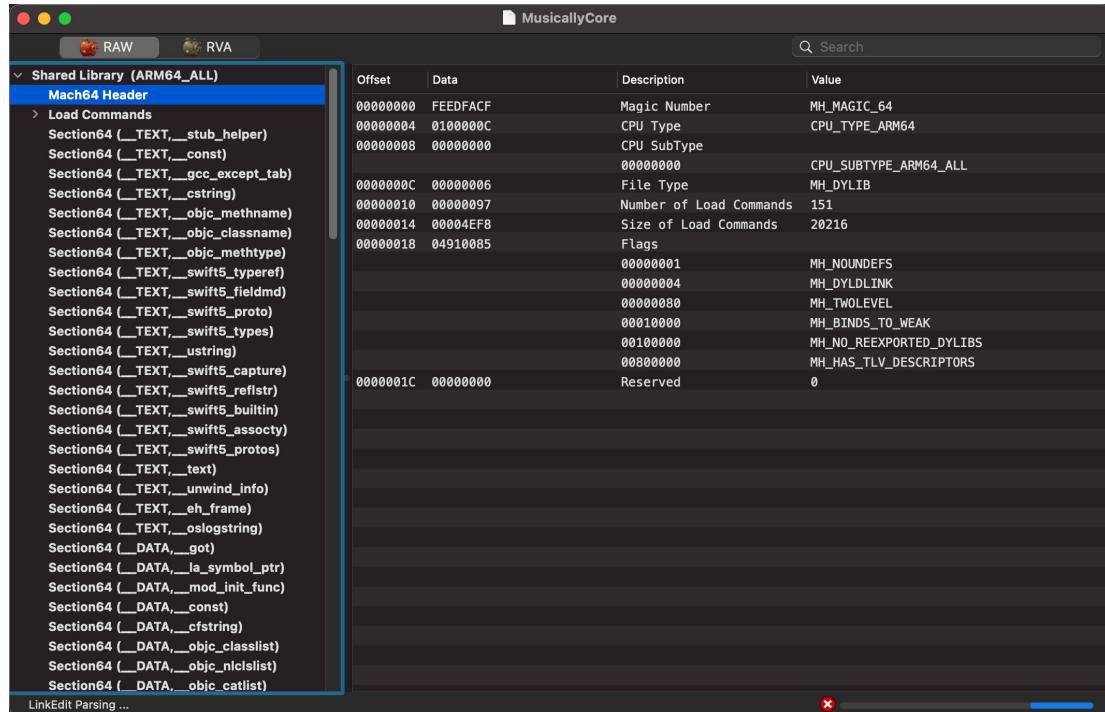
- MachOView
- rabin2
- jtool2
- otool
- pagestuff
- 其他
 - otool
 - 介绍: otool is a tool which interfaces with MachO binaries in order to insert/remove load commands, strip code signatures, resign, and remove aslr
 - 主页
 - <https://github.com/alexzielenski/optool>

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 15:57:22

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](https://github.com/fangshufeng/MachOView), 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:



crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:38:16

MachOView用法举例

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:30:06

main_arm64

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

Mach64 Header

| Offset | Data | Description | Value |
|----------|----------|-------------------------|--|
| 00000000 | FEEDFACF | Magic Number | MH_MAGIC_64 |
| 00000004 | 0100000C | CPU Type | CPU_TYPE_ARM64 |
| 00000008 | 00000000 | CPU SubType | 00000000 |
| 0000000C | 00000002 | File Type | MH_EXECUTE |
| 00000010 | 00000011 | Number of Load Commands | 17 |
| 00000014 | 000005B8 | Size of Load Commands | 1464 |
| 00000018 | 00200085 | Flags | 00000001
00000004
00000080
00200000 |
| 0000001C | 00000000 | Reserved | 0 |

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_PIE
- Reserved: 0

Load Commands

main_arm64

The screenshot shows the Binary Ninja interface with the file "main_arm64" open. The left pane displays a hierarchical tree of load commands under the "Executable (ARM64_ALL)" section. The "Load Commands" section is expanded, showing various entries like LC_SEGMENT_64, LC_DYLD_INFO_ONLY, and LC_CODE_SIGNATURE. The right pane is a table with columns: pFile, Data LO, Data HI, and Value. It lists numerous entries corresponding to the load commands in the tree, such as LC_SEGMENT_64 entries for PAGEZERO, TEXT, and DATA sections.

| pFile | Data LO | Data HI | Value |
|----------|-------------------------|-------------------------|------------------|
| 00000020 | 19 00 00 00 48 00 00 00 | 5F 5F 50 41 47 45 5A 45 |H...__PAGEZE |
| 00000030 | 52 4F 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | RO..... |
| 00000040 | 00 00 00 00 01 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000050 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000060 | 00 00 00 00 00 00 00 00 | 19 00 00 00 D8 01 00 00 | |
| 00000070 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 00000080 | 00 00 00 00 01 00 00 00 | 00 40 00 00 00 00 00 00 |@.... |
| 00000090 | 00 00 00 00 00 00 00 00 | 00 40 00 00 00 00 00 00 |@.... |
| 000000A0 | 05 00 00 00 05 00 00 00 | 05 00 00 00 00 00 00 00 | |
| 000000B0 | 5F 5F 74 65 78 74 00 00 | 00 00 00 00 00 00 00 00 | _text..... |
| 000000C0 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 000000D0 | 94 3B 00 00 01 00 00 00 | A0 02 00 00 00 00 00 00 | .;..... |
| 000000E0 | 94 3B 00 00 02 00 00 00 | 00 00 00 00 00 00 00 00 | .;..... |
| 000000F0 | 00 04 00 80 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000100 | 5F 5F 73 74 75 62 73 00 | 00 00 00 00 00 00 00 00 | _stubs..... |
| 00000110 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 00000120 | 34 3E 00 00 01 00 00 00 | 30 00 00 00 00 00 00 00 | 4>....0..... |
| 00000130 | 34 3E 00 00 02 00 00 00 | 00 00 00 00 00 00 00 00 | 4>.... |
| 00000140 | 08 04 00 80 00 00 00 00 | 0C 00 00 00 00 00 00 00 | |
| 00000150 | 5F 5F 73 74 75 62 5F 68 | 65 6C 70 65 72 00 00 00 | _stub_helper... |
| 00000160 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 00000170 | 64 3E 00 00 01 00 00 00 | 48 00 00 00 00 00 00 00 | d>....H..... |
| 00000180 | 64 3E 00 00 02 00 00 00 | 00 00 00 00 00 00 00 00 | d>.... |
| 00000190 | 00 04 00 80 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 000001A0 | 5F 5F 63 73 74 72 69 6E | 67 00 00 00 00 00 00 00 | _cstring..... |
| 000001B0 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 000001C0 | AC 3E 00 00 01 00 00 00 | 03 01 00 00 00 00 00 00 | >..... |
| 000001D0 | AC 3E 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | >..... |
| 000001E0 | 02 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 000001F0 | 5F 5F 75 6E 77 69 6E 64 | 5F 69 6E 66 6F 00 00 00 | _ unwind_info... |
| 00000200 | 5F 5F 54 45 58 54 00 00 | 00 00 00 00 00 00 00 00 | _TEXT..... |
| 00000210 | B0 3F 00 00 01 00 00 00 | 50 00 00 00 00 00 00 00 | .?....P..... |
| 00000220 | B0 3F 00 00 02 00 00 00 | 00 00 00 00 00 00 00 00 | .?..... |
| 00000230 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000240 | 19 00 00 00 98 00 00 00 | 5F 5F 44 41 54 41 5F 43 |__DATA_C |
| 00000250 | 4F 4E 53 54 00 00 00 00 | 00 40 00 00 01 00 00 00 | ONST....@..... |

LC_SEGMENT_64 (__PAGEZERO)

main_arm64

| Offset | Data | Description | Value |
|----------|----------------------------|-----------------------|---------------|
| 00000020 | 00000019 | Command | LC_SEGMENT_64 |
| 00000024 | 00000048 | Command Size | 72 |
| 00000028 | 5F5F504147455A45524F000... | Segment Name | __PAGEZERO |
| 00000038 | 0000000000000000 | VM Address | 0 |
| 00000040 | 00000010000000 | VM Size | 4294967296 |
| 00000048 | 0000000000000000 | File Offset | 0 |
| 00000050 | 0000000000000000 | File Size | 0 |
| 00000058 | 00000000 | Maximum VM Protection | 00000000 |
| | | VM PROT NONE | |
| 0000005C | 00000000 | Initial VM Protection | 00000000 |
| | | VM PROT NONE | |
| 00000060 | 00000000 | Number of Sections | 0 |
| 00000064 | 00000000 | Flags | |

LC_SEGMENT_64 (__TEXT)

main_arm64

| | Offset | Data | Description | Value |
|---|----------|----------------------------------|-----------------------|---------------|
| Executable (ARM64_ALL) | 00000068 | 00000019 | Command | LC_SEGMENT_64 |
| Mach64 Header | 0000006C | 000001D8 | Command Size | 472 |
| Load Commands | 00000070 | 5F554455854000000000000000000000 | Segment Name | __TEXT |
| LC_SEGMENT_64 (__PAGEZERO) | 00000080 | 0000000100000000 | VM Address | 4294967296 |
| LC_SEGMENT_64 (__TEXT) | 00000088 | 0000000000004000 | VM Size | 16384 |
| Section64 Header (__text) | 00000090 | 0000000000000000 | File Offset | 0 |
| Section64 Header (__stubs) | 00000098 | 0000000000004000 | File Size | 16384 |
| Section64 Header (__stub_helper) | 000000A0 | 00000005 | Maximum VM Protection | |
| Section64 Header (__cstring) | | 00000001 | VM PROT_READ | |
| Section64 Header (__ unwind_info) | | 00000004 | VM PROT_EXECUTE | |
| LC_SEGMENT_64 (__DATA_CONST) | 000000A4 | 00000005 | Initial VM Protection | |
| LC_SEGMENT_64 (__DATA) | | 00000001 | VM PROT_READ | |
| LC_SEGMENT_64 (__LINKEDIT) | | 00000004 | VM PROT_EXECUTE | |
| LC_DYLD_INFO_ONLY | 000000AB | 00000005 | Number of Sections | 5 |
| LC_SYMTAB | 000000AC | 00000000 | Flags | |
| 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 | | | | |

__TEXT, __text

main_arm64

The screenshot shows the Binary Ninja interface with the file 'main_arm64' loaded. The left sidebar displays the Mach-O header structure, while the main pane shows the detailed contents of the '_text' section.

| Offset | Data | Description | Value |
|----------|-----------------------------|-----------------------|--------------------------------------|
| 000000B0 | 5F5F74657874000000000000... | Section Name | _text |
| 000000C0 | 5F5F54558540000000000000... | Segment Name | _TEXT |
| 000000D0 | 000000100003B94 | Address | 4294982548 |
| 000000D8 | 000000000000002A0 | 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
80000000
00000400 |
| 000000F4 | 00000000 | Reserved1 | 0 |
| 000000F8 | 00000000 | Reserved2 | 0 |
| 000000FC | 00000000 | Reserved3 | 0 |

__TEXT, __stubs

main_arm64

Raw RVA

Executable (ARM64_ALL)

| Offset | Data | Description | Value |
|----------|-----------------------------|-----------------------|----------------------------------|
| 00000100 | 5F5F73747562730000000000... | Section Name | __stubs |
| 00000110 | 5F5F445585400000000000... | Segment Name | __TEXT |
| 00000120 | 0000000100003E34 | Address | 4294983220 |
| 00000128 | 00000000000000000030 | Size | 48 |
| 00000130 | 00003E34 | Offset | 15924 |
| 00000134 | 00000002 | Alignment | 4 |
| 00000138 | 00000000 | Relocations Offset | 0 |
| 0000013C | 00000000 | Number of Relocations | 0 |
| 00000140 | 80000408 | Flags | 00000008
80000000
00000400 |
| 00000144 | 00000000 | Indirect Sym Index | 0 |
| 00000148 | 0000000C | Size of Stubs | 12 |
| 0000014C | 00000000 | Reserved3 | 0 |

__TEXT, __stub_helper

main_arm64

Executable (ARM64_ALL)

| Offset | Data | Description | Value |
|----------|---------------------------|-----------------------|--------------------------------------|
| 00000150 | 5F5F737475625F68656C706.. | Section Name | __stub_helper |
| 00000160 | 5F5F445585400000000000.. | Segment Name | __TEXT |
| 00000170 | 0000000100003E64 | Address | 4294983268 |
| 00000178 | 0000000000000048 | Size | 72 |
| 00000180 | 00003E64 | Offset | 15972 |
| 00000184 | 00000002 | Alignment | 4 |
| 00000188 | 00000000 | Relocations Offset | 0 |
| 0000018C | 00000000 | Number of Relocations | 0 |
| 00000190 | 80000400 | Flags |
00000000
80000000
00000400 |
| 00000194 | 00000000 | Reserved1 | 0 |
| 00000198 | 00000000 | Reserved2 | 0 |
| 0000019C | 00000000 | Reserved3 | 0 |

__TEXT, __cstring

main_arm64

| Offset | Data | Description | Value |
|----------|----------------------------|-----------------------|------------|
| 000001A0 | 5F5F63737472696E6700000... | Section Name | __cstring |
| 000001B0 | 5FF545585400000000000... | Segment Name | __TEXT |
| 000001C0 | 000000100003EAC | Address | 4294983340 |
| 000001C8 | 0000000000000000103 | Size | 259 |
| 000001D0 | 00003EAC | Offset | 16044 |
| 000001D4 | 00000000 | Alignment | 1 |
| 000001D8 | 00000000 | Relocations Offset | 0 |
| 000001DC | 00000000 | Number of Relocations | 0 |
| 000001E0 | 00000002 | Flags | 00000002 |
| 000001E4 | 00000000 | Reserved1 | 0 |
| 000001E8 | 00000000 | Reserved2 | 0 |
| 000001EC | 00000000 | Reserved3 | 0 |

__TEXT, __unwind_info

main_arm64

Executable (ARM64_ALL)

| Offset | Data | Description | Value |
|----------|----------------------------|-----------------------|--------------------|
| 000001F0 | 5F5F756E77696E645F696E6... | Section Name | __ unwind_info |
| 00000200 | 5FF54558540000000000... | Segment Name | __TEXT |
| 00000210 | 0000000100003FB0 | Address | 4294983600 |
| 00000218 | 0000000000000050 | Size | 80 |
| 00000220 | 00003FB0 | Offset | 16304 |
| 00000224 | 00000002 | Alignment | 4 |
| 00000228 | 00000000 | Relocations Offset | 0 |
| 0000022C | 00000000 | Number of Relocations | 0 |
| 00000230 | 00000000 | Flags | 00000000 S_REGULAR |
| 00000234 | 00000000 | Reserved1 | 0 |
| 00000238 | 00000000 | Reserved2 | 0 |
| 0000023C | 00000000 | Reserved3 | 0 |

LC_SEGMENT_64 (__DATA_CONST)

main_arm64

| Offset | Data | Description | Value |
|----------|----------------------------|-----------------------|---------------|
| 00000240 | 00000019 | Command | LC_SEGMENT_64 |
| 00000244 | 00000098 | Command Size | 152 |
| 00000248 | 5F5F444154415F434F4E535... | Segment Name | __DATA_CONST |
| 00000258 | 0000000100004000 | VM Address | 4294983680 |
| 00000260 | 0000000000004000 | VM Size | 16384 |
| 00000268 | 0000000000004000 | File Offset | 16384 |
| 00000270 | 0000000000004000 | File Size | 16384 |
| 00000278 | 00000003 | Maximum VM Protection | |
| | 00000001 | VM PROT_READ | |
| | 00000002 | VM PROT_WRITE | |
| 0000027C | 00000003 | Initial VM Protection | |
| | 00000001 | VM PROT_READ | |
| | 00000002 | VM PROT_WRITE | |
| 00000280 | 00000001 | Number of Sections | 1 |
| 00000284 | 00000010 | Flags | |

__DATA_CONST, __got

main_arm64

The screenshot shows the Binary Ninja interface with the file 'main_arm64' open. The left pane displays the 'Load Commands' tree view, which is expanded to show various linker commands. The 'LC_SEGMENT_64 (__DATA)' command is currently selected, indicated by a blue highlight. The right pane shows a table of memory segments with columns for Offset, Data, Description, and Value. One row in the table corresponds to the selected segment, showing its address, size, and other details.

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|--------------|
| 00000288 | 5F5F676F740000000000000000000000 | Section Name | __got |
| 00000298 | 5F5F444154415F434F4E535400000000 | Segment Name | __DATA_CONST |
| 000002A8 | 0000000100004000 | Address | 4294983680 |
| 000002B0 | 0000000000000008 | Size | 8 |
| 000002B8 | 00004000 | Offset | 16384 |
| 000002BC | 00000003 | Alignment | 8 |
| 000002C0 | 00000000 | Relocations Offset | 0 |
| 000002C4 | 00000000 | Number of Relocations | 0 |
| 000002C8 | 00000006 | Flags | 00000006 |
| 000002CC | 00000004 | Indirect Sym Index | 4 |
| 000002D0 | 00000000 | Reserved2 | 0 |
| 000002D4 | 00000000 | Reserved3 | 0 |

LC_SEGMENT_64 (__DATA)

main_arm64

The screenshot shows the lief debugger interface with the file 'main_arm64' loaded. The left pane displays the Mach-O header and load commands. The right pane shows a detailed table of the load command entries.

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|---------------|
| 000002D8 | 00000019 | Command | LC_SEGMENT_64 |
| 000002DC | 00000138 | Command Size | 312 |
| 000002E0 | 5F5F4441544100000000000000000000 | Segment Name | __DATA |
| 000002F0 | 0000000100008000 | VM Address | 4295000064 |
| 000002F8 | 0000000000004000 | VM Size | 16384 |
| 00000300 | 0000000000008000 | File Offset | 32768 |
| 00000308 | 0000000000004000 | File Size | 16384 |
| 00000310 | 00000003 | Maximum VM Protection | |
| | 00000001 | VM PROT_READ | |
| | 00000002 | VM PROT_WRITE | |
| 00000314 | 00000003 | Initial VM Protection | |
| | 00000001 | VM PROT_READ | |
| | 00000002 | VM PROT_WRITE | |
| 00000318 | 00000003 | Number of Sections | 3 |
| 0000031C | 00000000 | Flags | |

__DATA, __la_symbol_ptr

main_arm64

| | Offset | Data | Description | Value |
|--------------------------------------|----------|----------------------------------|-----------------------|---------------------------------|
| Executable (ARM64_ALL) | 00000320 | 5F5F6C615F73796D626F6C5F70747200 | Section Name | _la_symbol_ptr |
| Mach64 Header | 00000330 | 5FF44154410000000000000000000000 | Segment Name | __DATA |
| Load Commands | 00000340 | 000000100008000 | Address | 4295000064 |
| LC_SEGMENT_64 (__PAGEZERO) | 00000348 | 00000000000000000000000000000000 | Size | 32 |
| > LC_SEGMENT_64 (__TEXT) | 00000350 | 00008000 | Offset | 32768 |
| > LC_SEGMENT_64 (__DATA_CONST) | 00000354 | 00000003 | Alignment | 8 |
| > LC_SEGMENT_64 (__DATA) | 00000358 | 00000000 | Relocations Offset | 0 |
| Section64 Header (_la_symbol_ptr) | 0000035C | 00000000 | Number of Relocations | 0 |
| Section64 Header (_data) | 00000360 | 00000007 | Flags | 00000007 S_LAZY_SYMBOL_POINTERS |
| Section64 Header (_common) | 00000364 | 00000005 | Indirect Sym Index | 5 |
| LC_SEGMENT_64 (__LINKEDIT) | 00000368 | 00000000 | Reserved2 | 0 |
| LC_DYLD_INFO_ONLY | 0000036C | 00000000 | Reserved3 | 0 |
| 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 | | | | |

__DATA, __data

main_arm64

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|------------|
| 00000370 | 5F5F6461746100000000000000000000 | Section Name | _data |
| 00000380 | 5FF44154410000000000000000000000 | Segment Name | _DATA |
| 00000390 | 000000100008020 | Address | 4295000096 |
| 00000398 | 0000000000000001C | Size | 28 |
| 000003A0 | 00000020 | Offset | 32800 |
| 000003A4 | 00000003 | Alignment | 8 |
| 000003A8 | 00000000 | Relocations Offset | 0 |
| 000003AC | 00000000 | Number of Relocations | 0 |
| 000003B0 | 00000000 | Flags | 00000000 |
| 000003B4 | 00000000 | Reserved1 | 0 |
| 000003B8 | 00000000 | Reserved2 | 0 |
| 000003BC | 00000000 | Reserved3 | 0 |

__DATA, __common

main_arm64

Executable (ARM64_ALL)

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|---------------------|
| 000003C0 | 5F5F636F6D6D6F6E0000000000000000 | Section Name | __common |
| 000003D0 | 5FF44154410000000000000000000000 | Segment Name | __DATA |
| 000003E0 | 00000010000803C | Address | 4295000124 |
| 000003E8 | 0000000000000004 | Size | 4 |
| 000003F0 | 00000000 | Offset | 0 |
| 000003F4 | 00000002 | Alignment | 4 |
| 000003FB | 00000000 | Relocations Offset | 0 |
| 000003FC | 00000000 | Number of Relocations | 0 |
| 00000400 | 00000001 | Flags | 00000001 S_ZEROINIT |
| 00000404 | 00000000 | Reserved1 | 0 |
| 00000408 | 00000000 | Reserved2 | 0 |
| 0000040C | 00000000 | Reserved3 | 0 |

LC_SEGMENT_64 (__LINKEDIT)

main_arm64

The screenshot shows the Binary Ninja interface with the file 'main_arm64' open. On the left, the navigation pane displays the executable structure, including sections like Mach64 Header, Load Commands, and various LC_ commands. The 'LC_SEGMENT_64 (__LINKEDIT)' command is currently selected. On the right, the memory dump view shows the raw data and its corresponding memory map.

| Offset | Data | Description | Value |
|----------|----------------------------------|-----------------------|---------------|
| 00000410 | 00000019 | Command | LC_SEGMENT_64 |
| 00000414 | 00000048 | Command Size | 72 |
| 00000418 | 5F5F4C494E4B45444954000000000000 | Segment Name | __LINKEDIT |
| 00000428 | 000000010000C000 | VM Address | 4295016448 |
| 00000430 | 0000000000004000 | VM Size | 16384 |
| 00000438 | 000000000000C000 | File Offset | 49152 |
| 00000440 | 0000000000004C7 | File Size | 1223 |
| 00000448 | 00000001 | Maximum VM Protection | 00000001 |
| | | VM PROT_READ | |
| 0000044C | 00000001 | Initial VM Protection | 00000001 |
| | | VM PROT_READ | |
| 00000450 | 00000000 | Number of Sections | 0 |
| 00000454 | 00000000 | Flags | |

LC_DYLD_INFO_ONLY

main_arm64

| 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 |

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_UID
 - ??? (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

LC_SYMTAB

main_arm64

The screenshot shows the Binary Ninja interface with the file 'main_arm64' open. The left pane displays a tree view of the load commands, and the right pane shows a table of command details.

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** (selected)
- LC_DYSYMTAB
- LC_LOAD_DYLINKER
- LC_UID
- ??? (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

Table:

| 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

main_arm64

| Offset | Data | Description | Value |
|----------|----------|--------------------------|-------------|
| 000004A0 | 0000000B | Command | LC_DYSYMTAB |
| 000004A4 | 00000050 | Command Size | 80 |
| 000004A8 | 00000000 | LocSymbol Index | 0 |
| 000004AC | 00000001 | LocSymbol Number | 1 |
| 000004B0 | 00000001 | Defined ExtSymbol Index | 1 |
| 000004B4 | 00000008 | Defined ExtSymbol Number | 8 |
| 000004B8 | 00000009 | Undef ExtSymbol Index | 9 |
| 000004BC | 00000005 | Undef ExtSymbol Number | 5 |
| 000004C0 | 00000000 | TOC Offset | 0 |
| 000004C4 | 00000000 | TOC Entries | 0 |
| 000004C8 | 00000000 | Module Table Offset | 0 |
| 000004CC | 00000000 | Module Table Entries | 0 |
| 000004D0 | 00000000 | ExtRef Table Offset | 0 |
| 000004D4 | 00000000 | ExtRef Table Entries | 0 |
| 000004D8 | 0000C1D8 | IndSym Table Offset | 49624 |
| 000004DC | 00000009 | IndSym Table Entries | 9 |
| 000004E0 | 00000000 | ExtReloc Table Offset | 0 |
| 000004E4 | 00000000 | ExtReloc Table Entries | 0 |
| 000004E8 | 00000000 | LocReloc Table Offset | 0 |
| 000004EC | 00000000 | LocReloc Table Entries | 0 |

LC_LOAD_DYLINKER

main_arm64

The screenshot shows the lief debugger interface with the file 'main_arm64' loaded. On the left, a tree view displays the executable's structure, including sections like Mach64 Header, Load Commands, and various segment headers. On the right, a table provides detailed information for each load command. The 'LC_LOAD_DYLINKER' command is highlighted with a blue selection bar.

| 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

main_arm64

The screenshot shows the Mach-O dump tool interface. On the left, a tree view displays various Mach-O command types. One node, 'LC_UUID', is highlighted with a blue selection bar at the bottom. On the right, a table provides detailed information for the selected command.

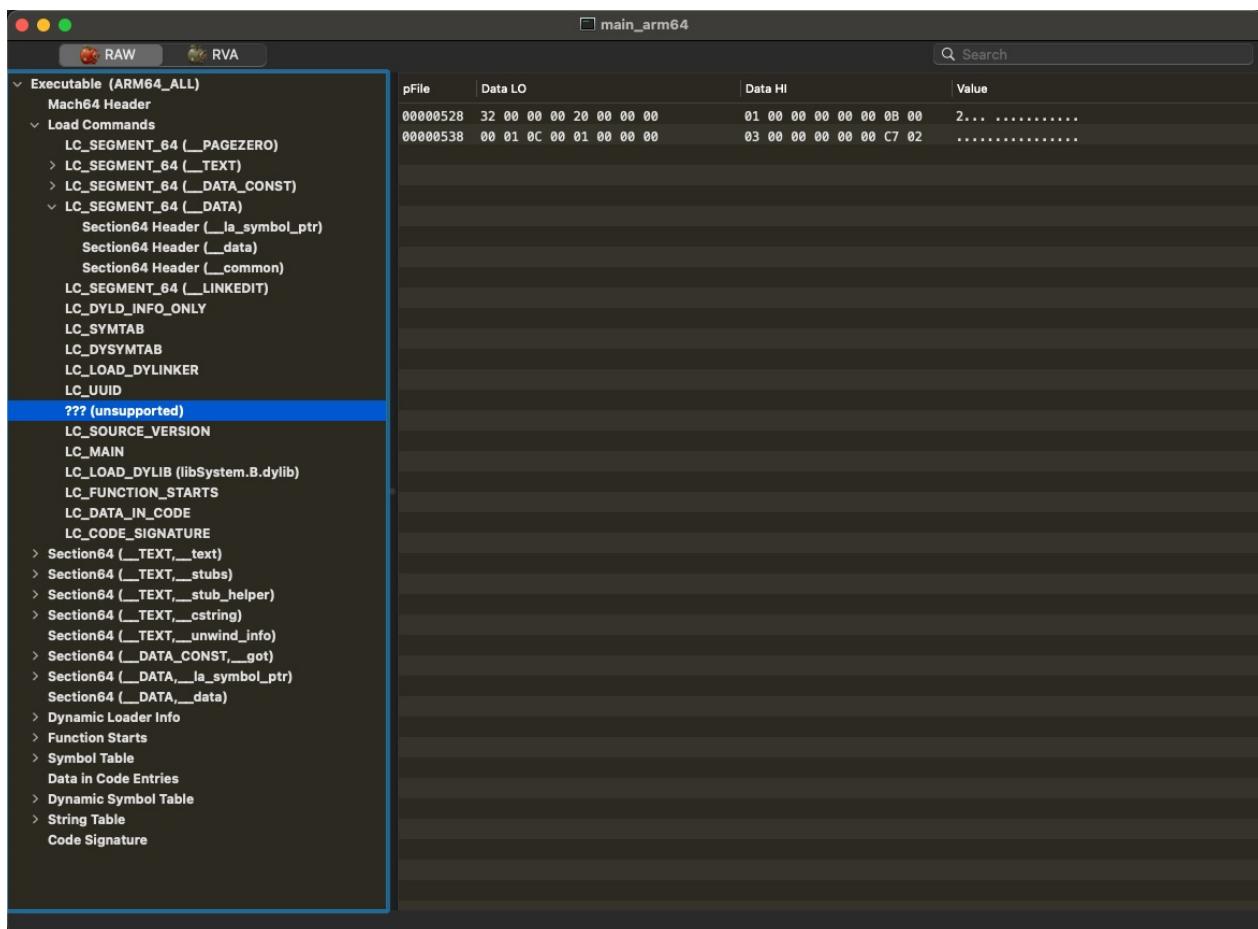
Table Headers:

| Offset | Data | Description | Value |
|--------|------|-------------|-------|
|--------|------|-------------|-------|

Table Data:

| | | | |
|----------|----------------------------------|--------------|--------------------------------------|
| 00000510 | 0000001B | Command | LC_UUID |
| 00000514 | 00000018 | Command Size | 24 |
| 00000518 | 204745F226AC32F7B23576DAEC17F5D9 | UUID | 204745F2-26AC-32F7-B235-76DAEC17F5D9 |

??? (unsupported)

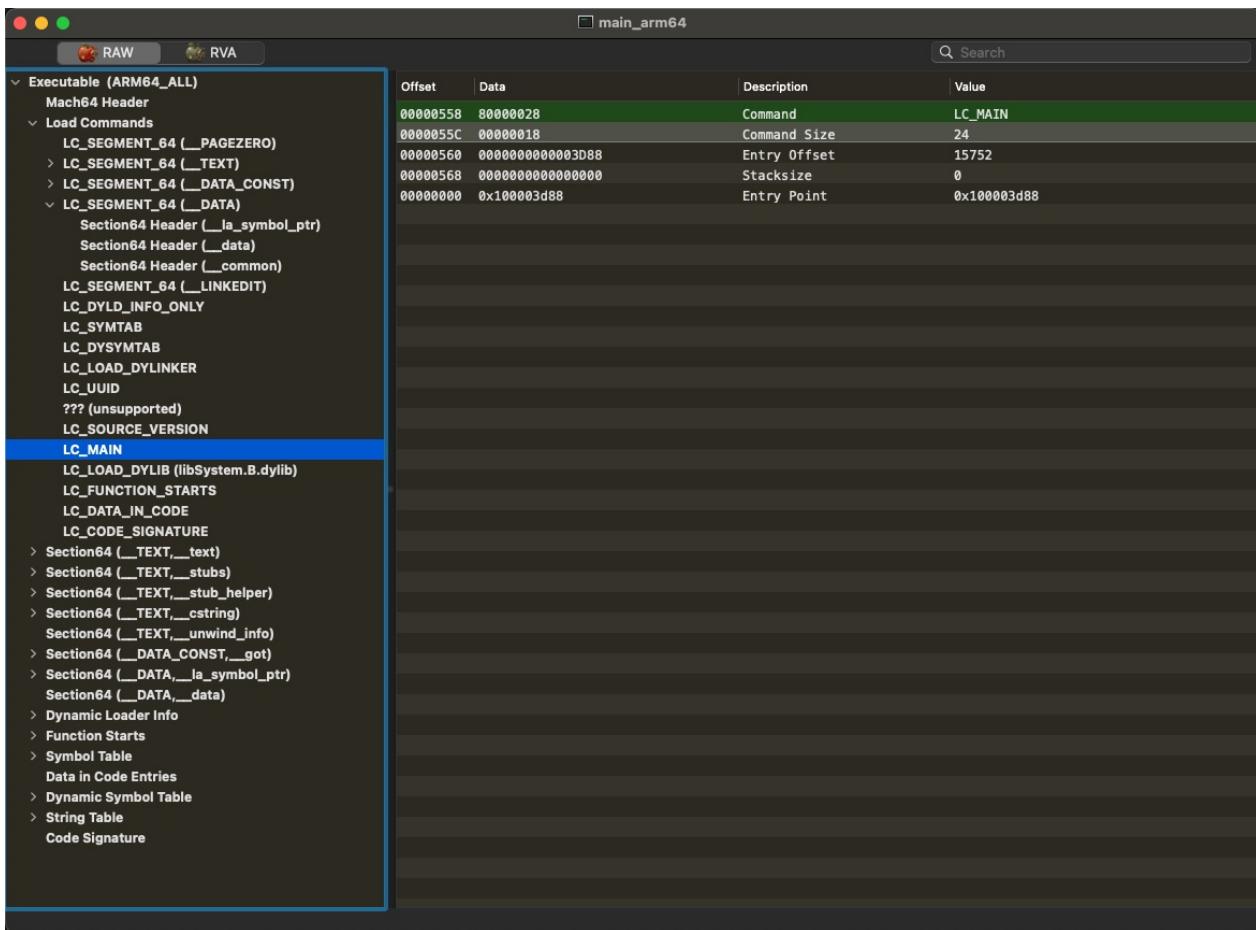


LC_SOURCE_VERSION

The screenshot shows the Mach-O dump tool interface. On the left, a tree view displays various load commands. The 'LC_SOURCE_VERSION' command is selected and highlighted with a blue border. On the right, a table provides detailed information about this command.

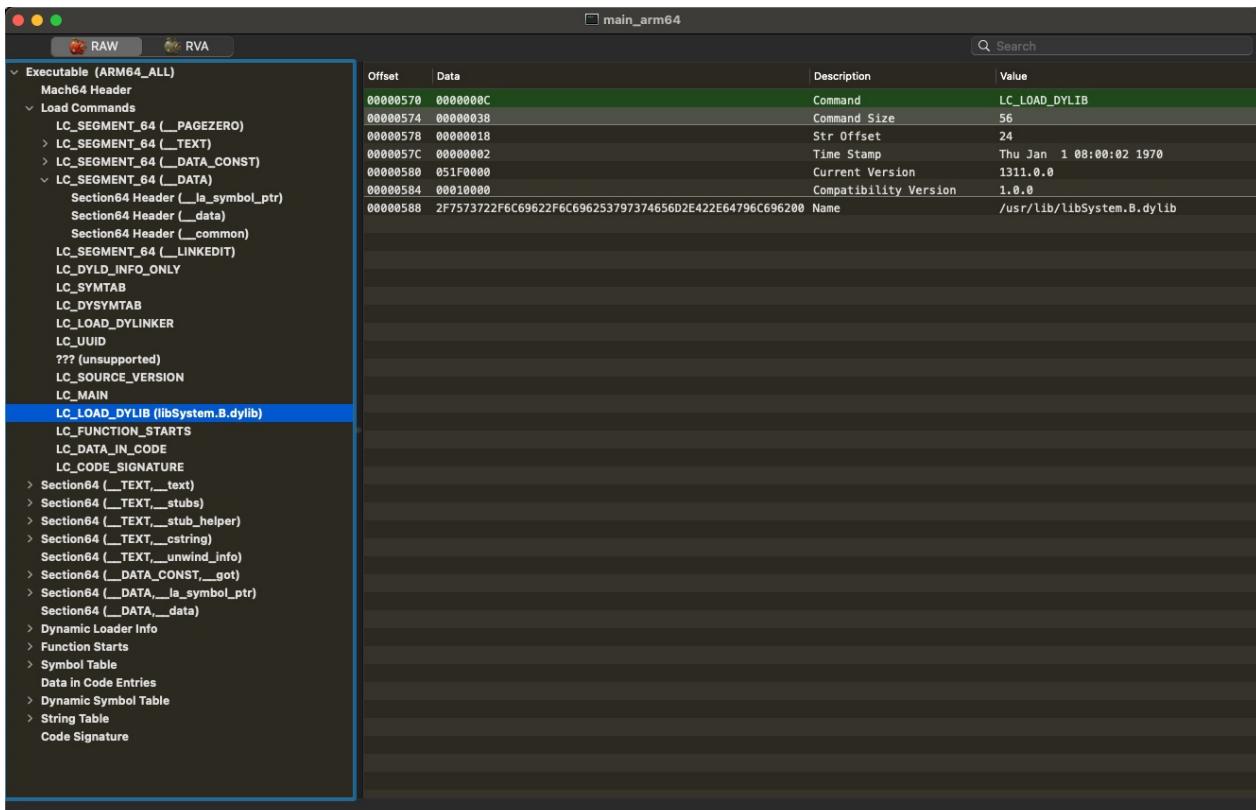
| Offset | Data | Description | Value |
|----------|------------------|--------------|-------------------|
| 00000548 | 0000002A | Command | LC_SOURCE_VERSION |
| 0000054C | 00000010 | Command Size | 16 |
| 00000550 | 0000000000000000 | Version | 0.0 |

LC_MAIN

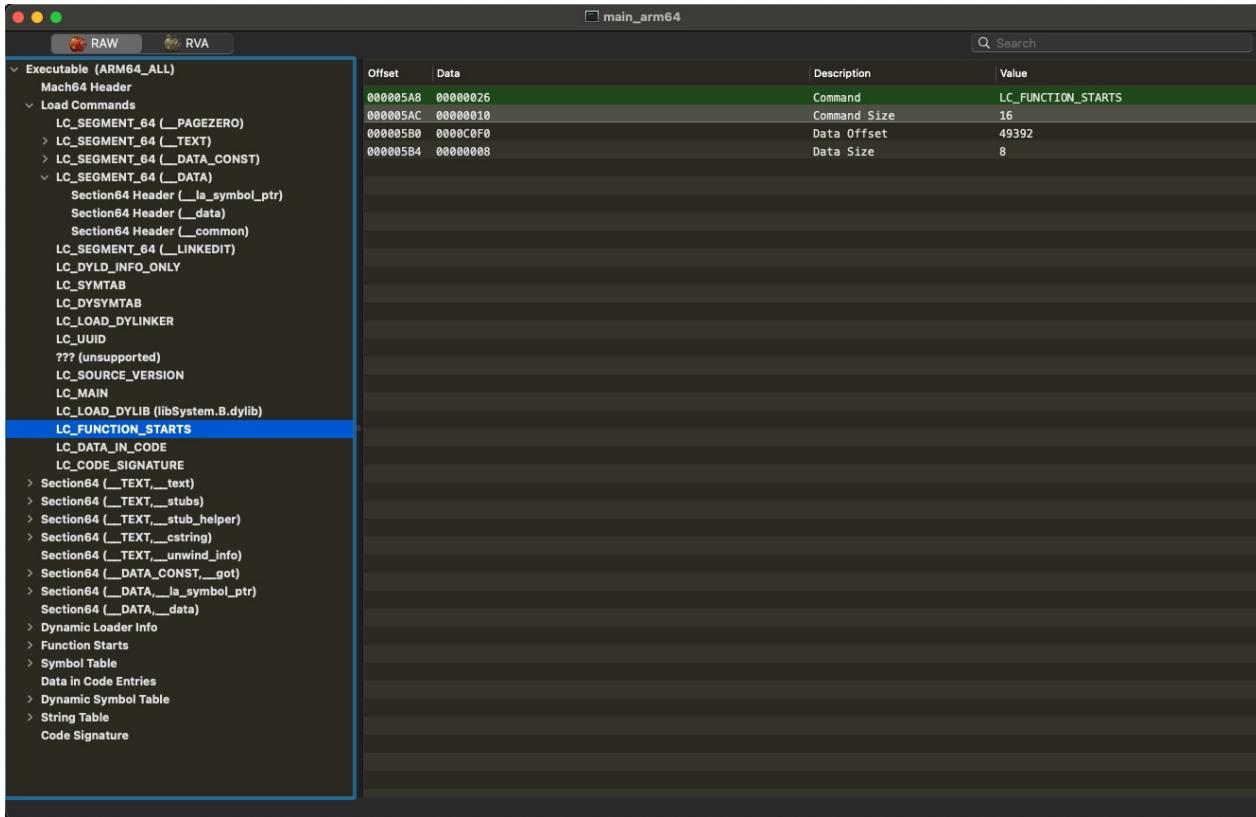


估计就是 入口函数 入口地址 = 一般叫做 main函数的地方了

LC_LOAD_DYLIB (libSystem.B.dylib)



LC_FUNCTION_STARTS

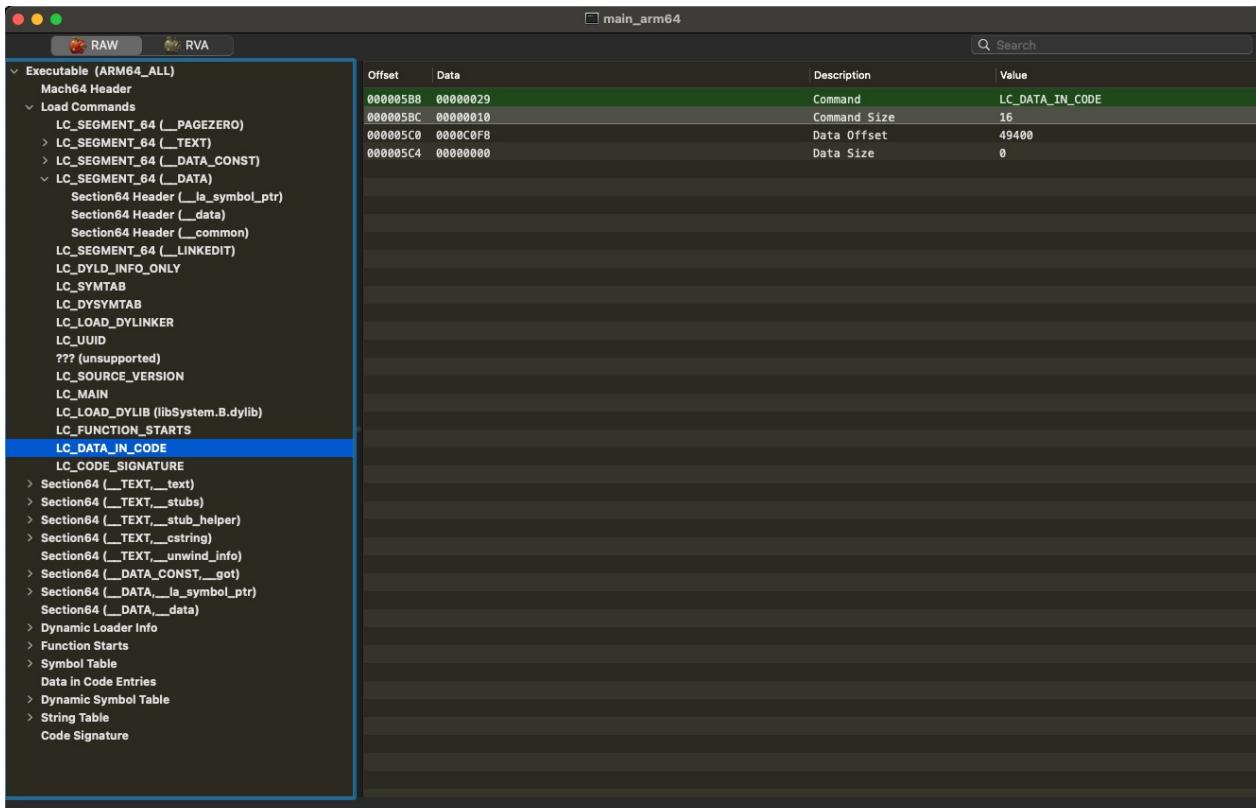


The screenshot shows the Mach-O debugger interface with the 'main_arm64' file open. The left pane displays a tree view of the Load Commands section under the Executable (ARM64_ALL) category. The 'LC_FUNCTION_STARTS' command is highlighted with a blue selection bar. The right pane shows a table of command details:

| Offset | Data | Description | Value |
|----------|----------|--------------|--------------------|
| 000005A8 | 00000026 | Command | LC_FUNCTION_STARTS |
| 000005AC | 00000010 | Command Size | 16 |
| 000005B0 | 0000C0F0 | Data Offset | 49392 |
| 000005B4 | 00000008 | Data Size | 8 |

好像是：需要启动运行的函数的列表？

LC_DATA_IN_CODE



The screenshot shows the Mach-O debugger interface with the 'main_arm64' file open. The left pane displays a tree view of the Load Commands section under the Executable (ARM64_ALL) category. The 'LC_DATA_IN_CODE' command is highlighted with a blue selection bar. The right pane shows a table of command details:

| Offset | Data | Description | Value |
|----------|----------|--------------|-----------------|
| 000005B8 | 00000029 | Command | LC_DATA_IN_CODE |
| 000005BC | 00000010 | Command Size | 16 |
| 000005C0 | 0000C0F8 | Data Offset | 49400 |
| 000005C4 | 00000000 | Data Size | 0 |

LC_CODE_SIGNATURE

Screenshot of the Mach-O dump tool showing the LC_CODE_SIGNATURE command.

Left Panel (Load Commands Tree):

- 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_DSYMTAB
 - 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

Sections

Section64 (__TEXT, __text)

Screenshot of the Mach-O dump tool showing the Section64 (__TEXT, __text) assembly code.

Left Panel (Section Tree):

- Executable (ARM64_ALL)
 - Mach64 Header
 - Load Commands
 - Section64 (__TEXT, __text)
 - Assembly
 - > 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

- Assembly

Screenshot of the Immunity Debugger showing assembly code for two sections: `Section64 (__TEXT, __text)` and `Section64 (__TEXT, __stubs)`.

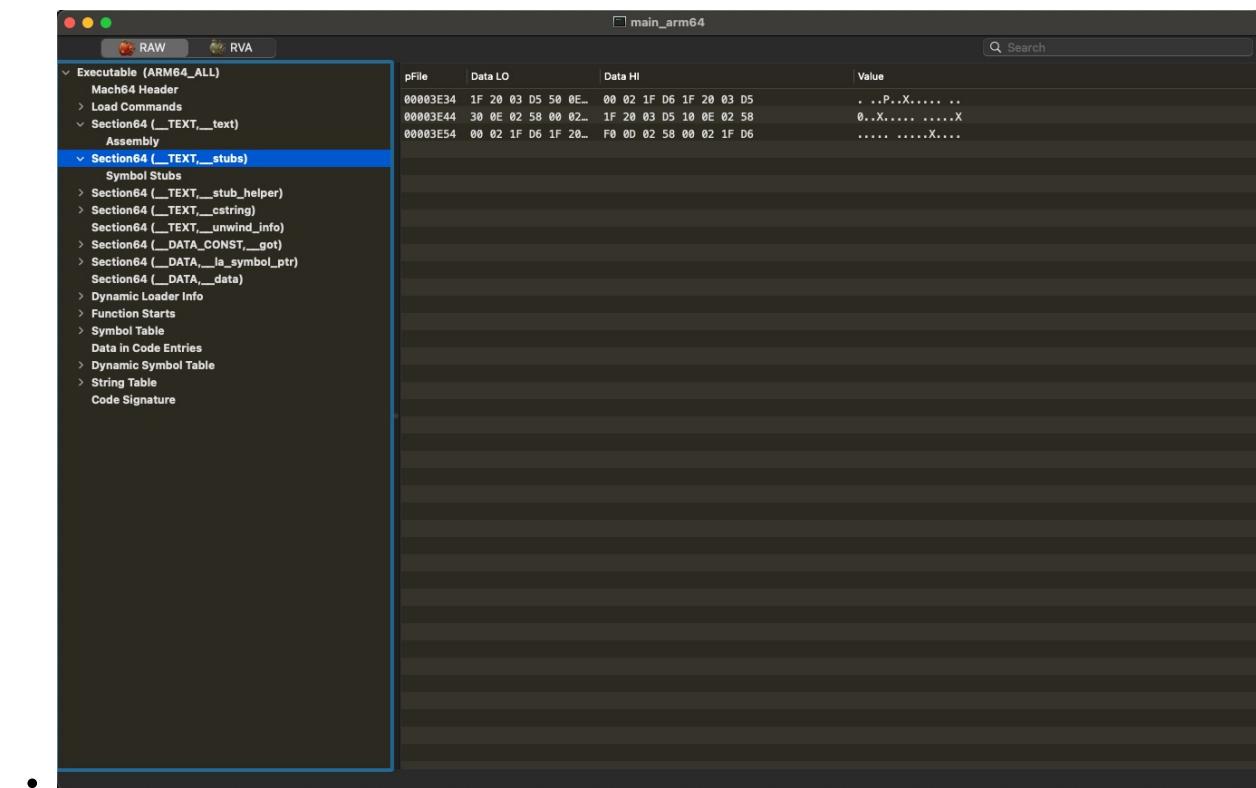
Section64 (__TEXT, __text)

| Offset | Data | Description | Value |
|----------|----------|----------------------|-------|
| 00003B94 | FFC30001 | sub sp, sp, #0x30 | |
| 00003B98 | EA33A089 | ldr v10, [sp, #0x30] | |
| 00003B9C | E9374089 | ldr v9, [sp, #0x34] | |
| 00003BA0 | E83B4089 | ldr v8, [sp, #0x38] | |
| 00003BA4 | E02F0089 | str v8, [sp, #0x2c] | |
| 00003BAA | E12B0089 | str v1, [sp, #0x28] | |
| 00003BAC | E2270089 | str v2, [sp, #0x24] | |
| 00003B99 | E3290089 | str v3, [sp, #0x20] | |
| 00003B84 | E41F0089 | str v4, [sp, #0x1c] | |
| 00003B88 | E51B0089 | str v5, [sp, #0x18] | |
| 00003B8C | E6170089 | str v6, [sp, #0x14] | |
| 00003B90 | E7130089 | str v7, [sp, #0x10] | |
| 00003B84 | EA0F0089 | str v10, [sp, #0xc] | |
| 00003B88 | E90B0089 | str v9, [sp, #8] | |
| 00003BCC | E8070089 | str v8, [sp, #4] | |
| 00003B00 | E92F0089 | ldr v8, [sp, #0x2c] | |
| 00003B04 | E92B0089 | ldr v9, [sp, #0x28] | |
| 00003B08 | 00109088 | add v8, w8, w9 | |
| 00003B0C | E9274089 | ldr v9, [sp, #0x24] | |
| 00003B80 | 00109088 | add v8, w8, w9 | |
| 00003B84 | E9234089 | ldr v9, [sp, #0x18] | |
| 00003B88 | 00109088 | add v8, w8, w9 | |
| 00003BEC | E91F4089 | ldr v9, [sp, #0x1c] | |
| 00003B90 | 00109088 | add v8, w8, w9 | |
| 00003BFA | E91B4089 | ldr v9, [sp, #0x18] | |
| 00003B98 | 00109088 | add v8, w8, w9 | |
| 00003BFC | E9174089 | ldr v9, [sp, #0x14] | |
| 00003C00 | 00109088 | add v8, w8, w9 | |
| 00003C04 | E9134089 | ldr v9, [sp, #0x10] | |
| 00003C08 | 00109088 | add v8, w8, w9 | |
| 00003C0C | E90F4089 | ldr v9, [sp, #0xc] | |
| 00003C10 | 00109088 | add v8, w8, w9 | |
| 00003C14 | E90B4089 | ldr v9, [sp, #8] | |
| 00003C18 | 00109088 | add v8, w8, w9 | |
| 00003C1C | E9074089 | ldr v9, [sp, #4] | |
| 00003C20 | 00109088 | add v8, w8, w9 | |
| 00003C24 | E8030089 | str v8, [sp] | |
| 00003C28 | E0034089 | ldr v0, [sp] | |
| 00003C2C | FFC30091 | add sp, sp, #0x30 | |

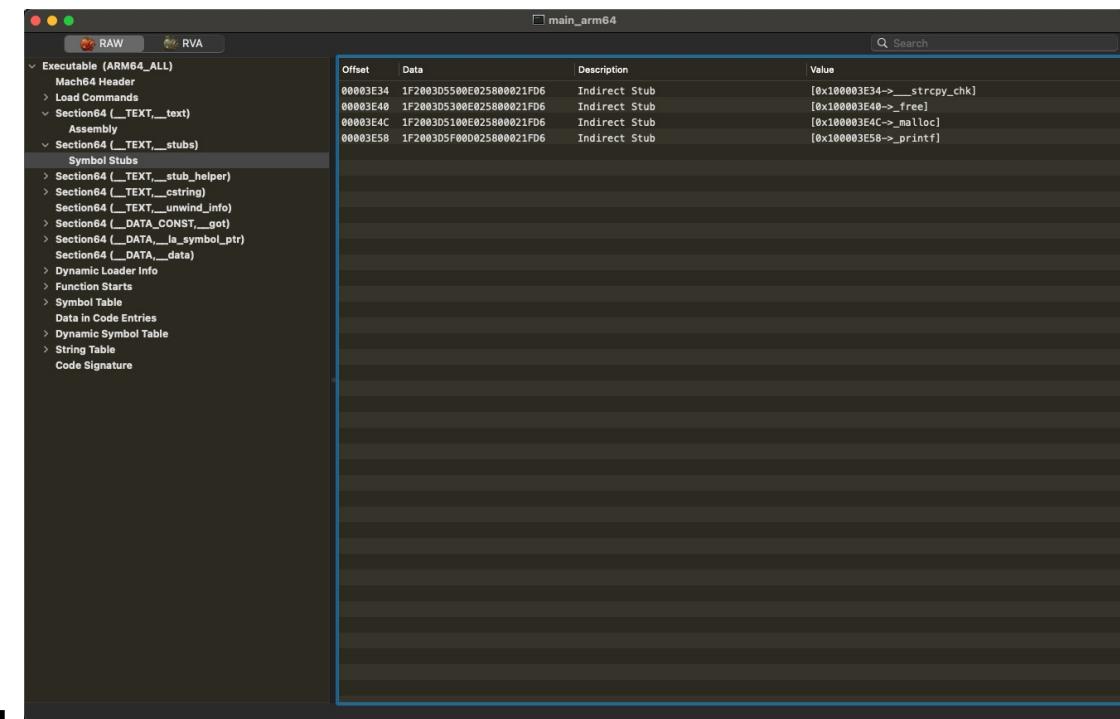
Section64 (__TEXT, __stubs)

| Offset | Data | Description | Value |
|----------|-----------|---------------------------------------|-------|
| 00003D94 | 00003D94 | stur v2r, [x29, #0x1111111111111111] | |
| 00003D98 | A0831F88 | stur v0, [x29, #0xfffffffffffff...] | |
| 00003D9C | A1831FF8 | stur x1, [x29, #0xfffffffffffff...] | |
| 00003DA0 | A9835F88 | ldur v9, [x29, #0xfffffffffffff...] | |
| 00003DA4 | E8B309AA | mov x8, x9 | |
| 00003DA8 | 00000090 | adrp x0, #0x100003000 | |
| 00003DAC | 00383E91 | add x0, x0, #0xf18e | |
| 00003DB0 | E9030091 | mov x9, sp | |
| 00003D84 | 280100F9 | str x8, [x9] | |
| 00003DB8 | 28000094 | bl #0x100003e58 | |
| 00003DC0 | BFC31EB8 | stur v2r, [x29, #0xfffffffffffff...] | |
| 00003DC0 | ABC35E88 | ldur v8, [x29, #0xfffffffffffff...] | |
| 00003DC4 | A9835F88 | ldur v9, [x29, #0xfffffffffffff...] | |
| 00003DC8 | 00810968 | subs v8, w8, w9 | |
| 00003DCC | 0A020054 | bge #0x100003e0c | |
| 00003DD0 | ABC35E88 | ldur v8, [x29, #0xfffffffffffff...] | |
| 00003D04 | EA0308AA | mov x10, x8 | |
| 00003D08 | A8B35FF8 | ldur x8, [x29, #0xfffffffffffff...] | |
| 00003D0C | 00930E88 | ldursw x9, [x29, #0xfffffffffffff...] | |
| 00003DE0 | 087969F8 | ldr x8, [x8, x9, lsl #3] | |
| 00003DE4 | 00000090 | adrp x0, #0x100003000 | |
| 00003DE8 | 005C3E91 | add x0, x0, #0xf97 | |
| 00003DEC | E9030091 | mov x9, sp | |
| 00003DF0 | 2A0100F9 | str x10, [x9] | |
| 00003DFA | 280500F9 | str x8, [x9, #8] | |
| 00003D98 | 18000094 | bl #0x100003e58 | |
| 00003D9C | ABC35E88 | ldur v8, [x29, #0xfffffffffffff...] | |
| 00003E00 | 008050011 | add v8, w8, #1 | |
| 00003E04 | A8C31EB8 | stur v8, [x29, #0xfffffffffffff...] | |
| 00003E08 | EEFFF117 | b #0x100003d08 | |
| 00003E0C | 28000052 | movz v8, #0x1 | |
| 00003E10 | 00010012 | and v0, w8, #1 | |
| 00003E14 | A1000052 | movz v1, #0x5 | |
| 00003E18 | 02000090 | adrp x2, #0x100003000 | |
| 00003E1C | A2903E91 | add x2, x2, #0xf14 | |
| 00003E20 | 85FFF97 | bl #0x100003c34 | |
| 00003E24 | 00000052 | movz v0, #0 | |
| 00003E28 | F07843A9 | ldp x29, x30, [sp, #0x30] | |
| 00003E2C | FF030191 | add sp, sp, #0x40 | |
| 00003E30 | C0035FD6 | ret | |

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

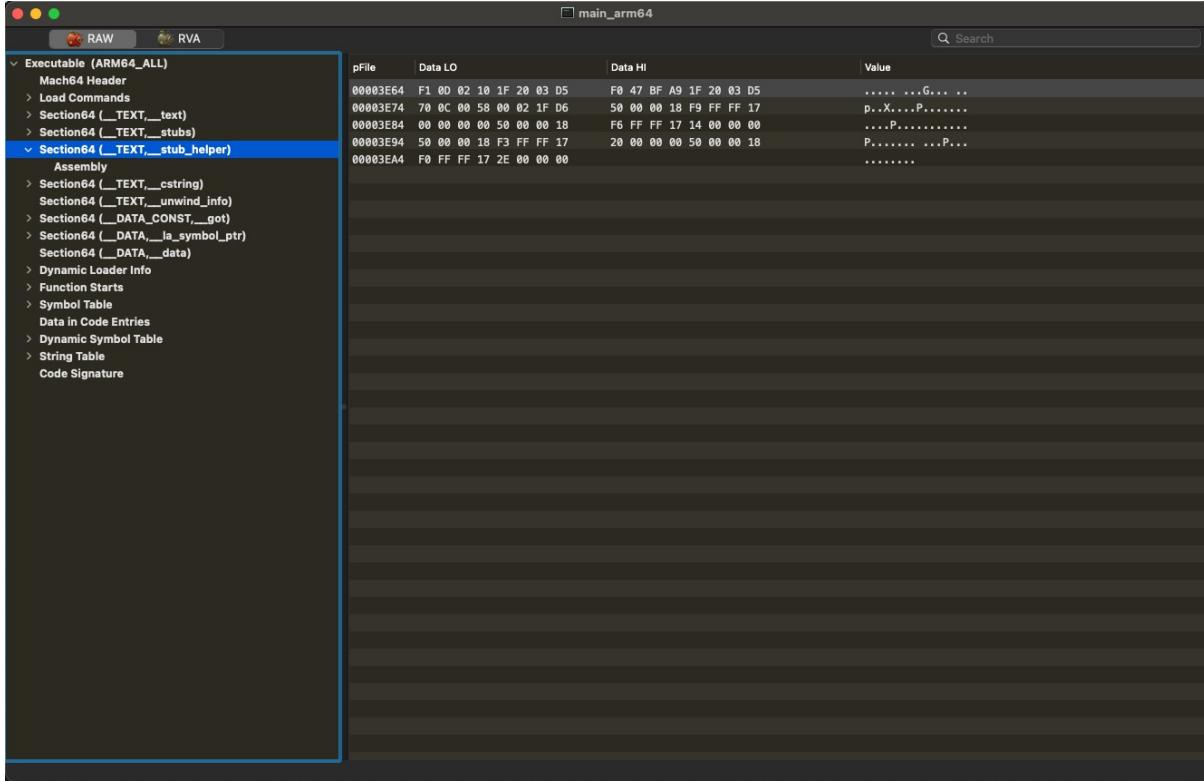
所以此处表示： 所引用的外部的函数

此处分别是：

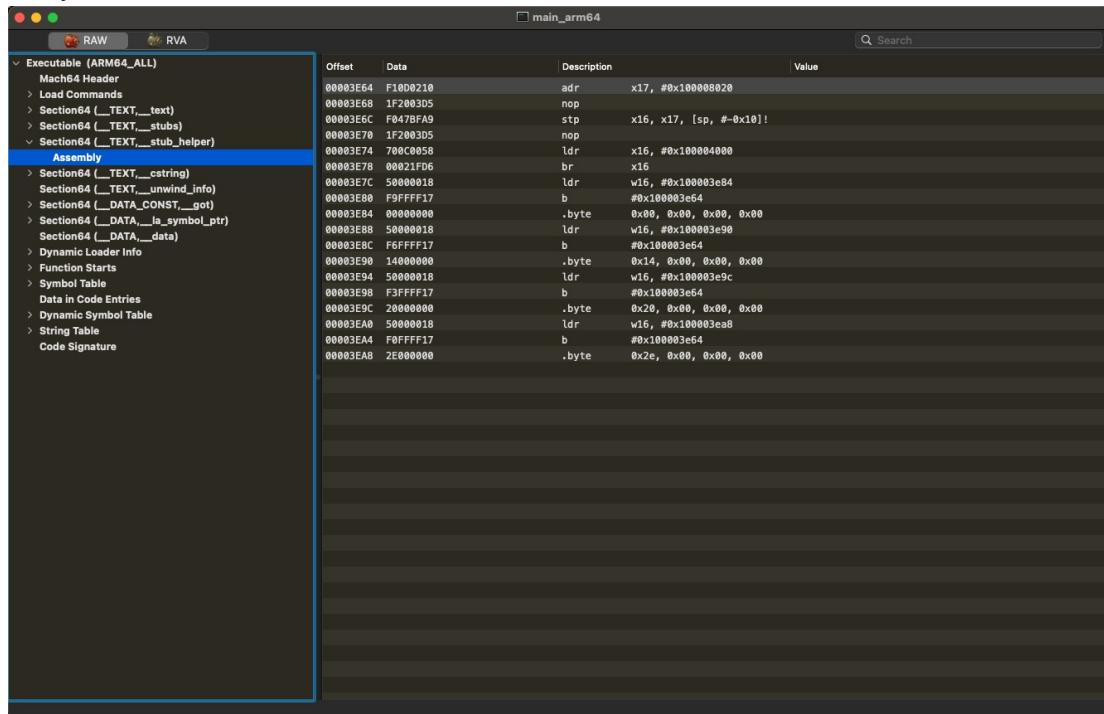
- `__strcpy_chk`

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

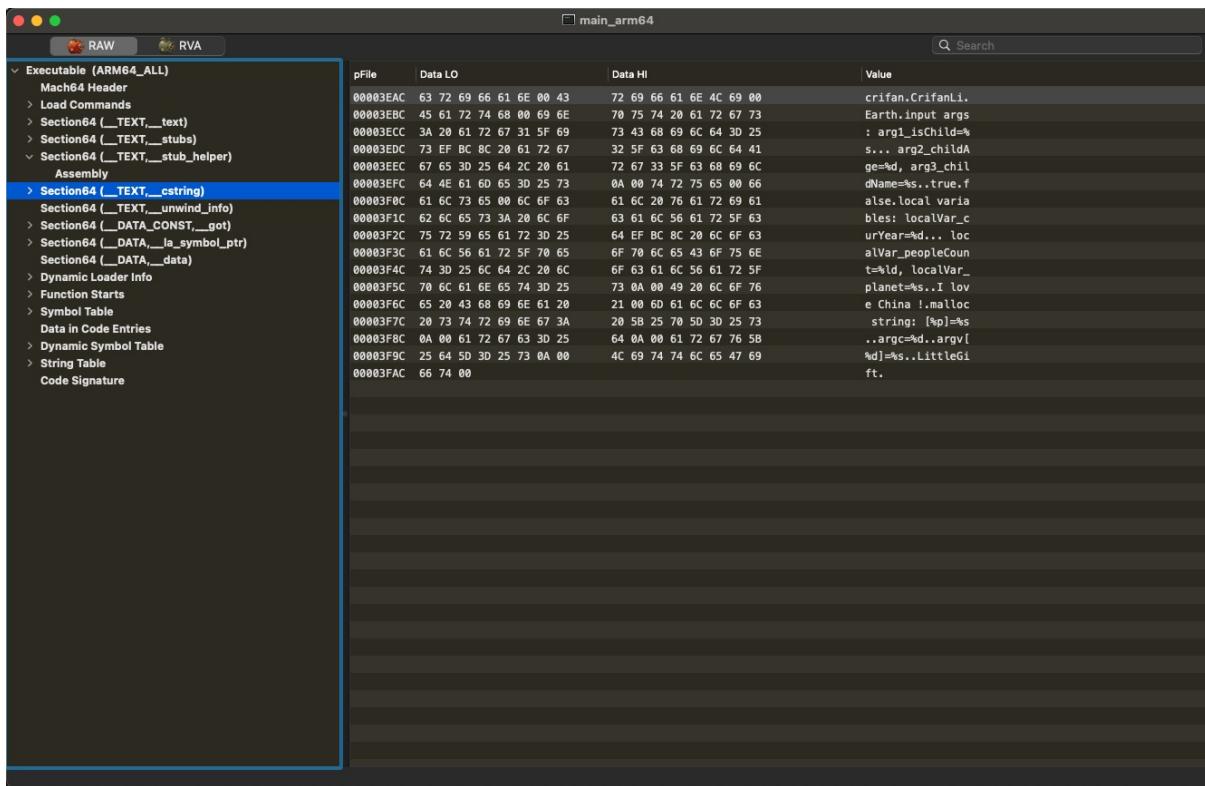
Section64 (`__TEXT,__stub_helper`)



- Assembly

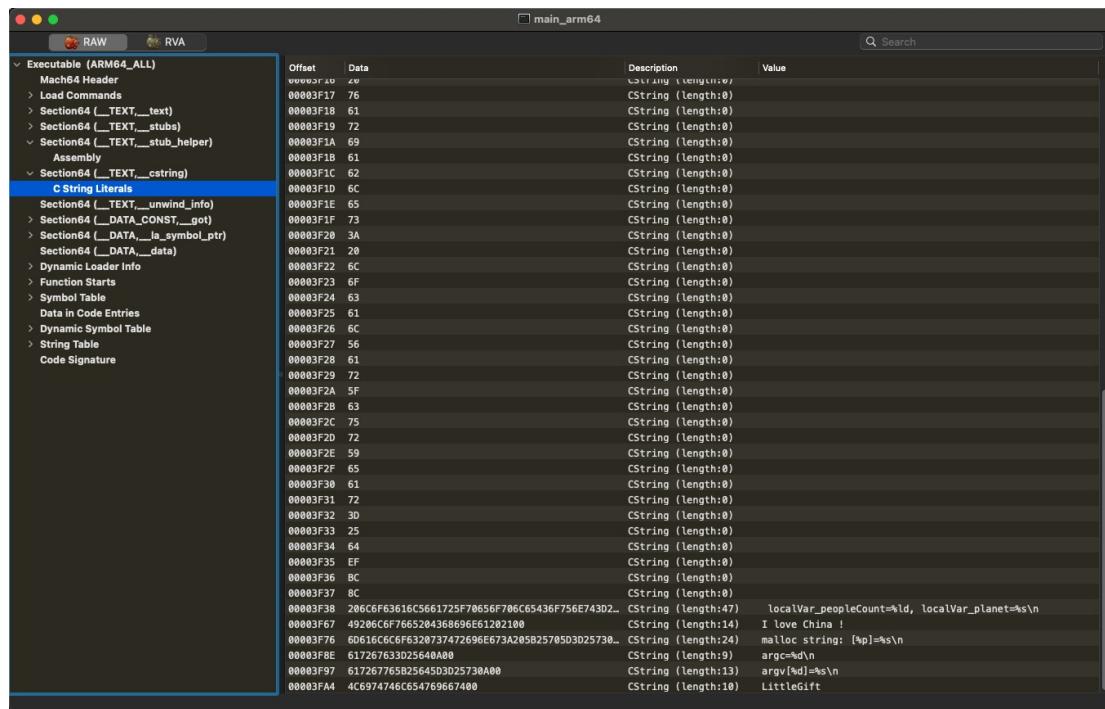


Section64 (`__TEXT,__cstring`)

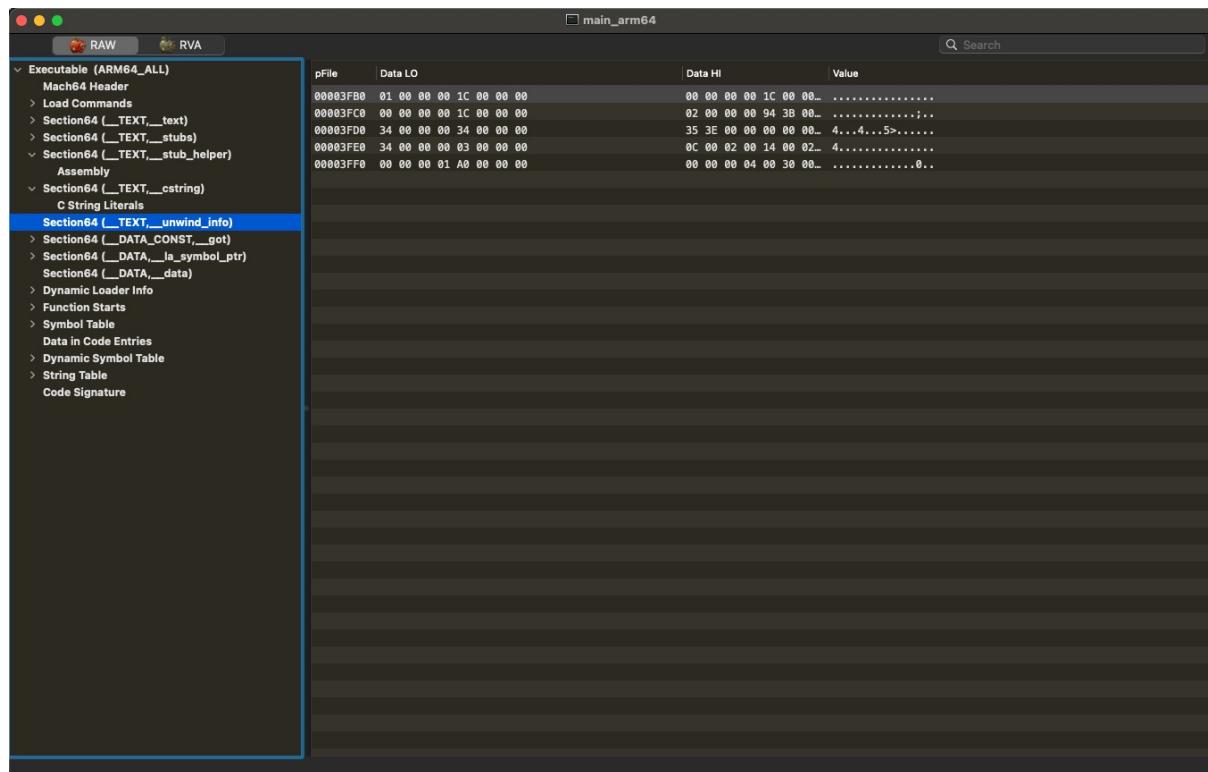


◦ C String Literals

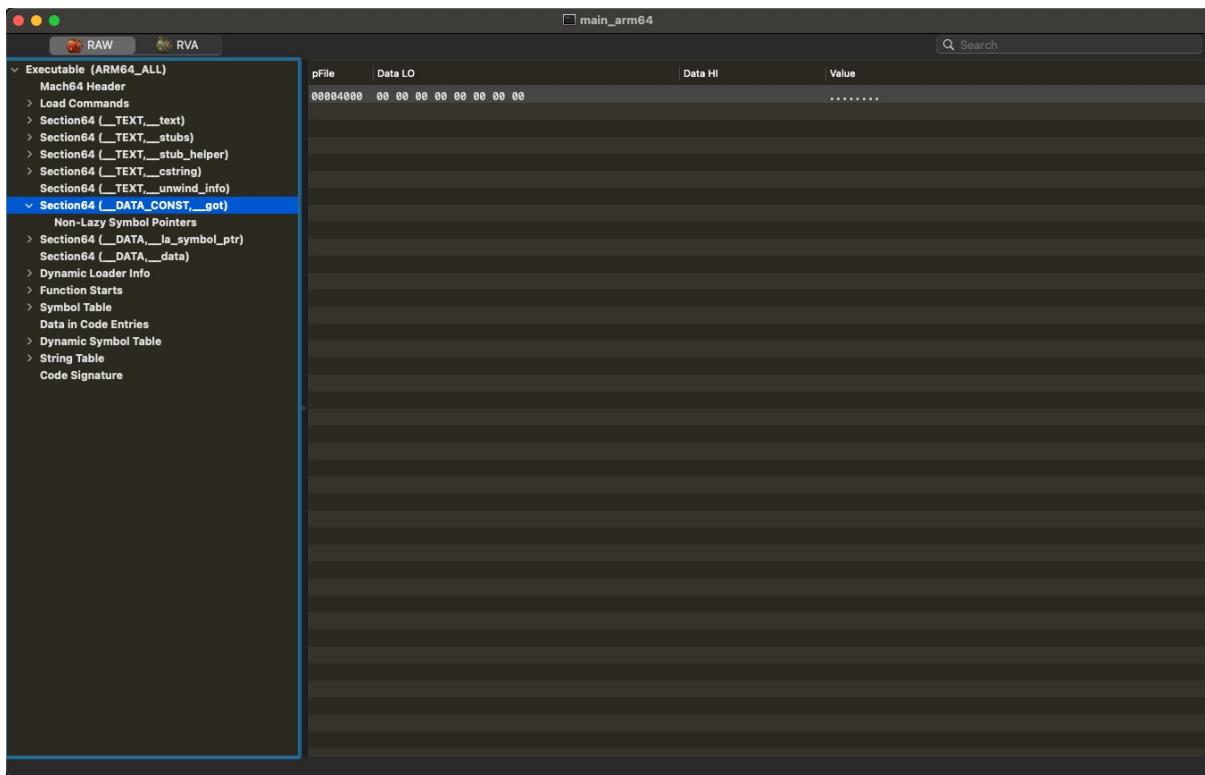
| Offset | Data | Description | Value |
|----------|--|---------------------|---------------------------------------|
| 00003EAC | 63726966616E00 | CString (length:6) | crifan |
| 00003EB3 | 43726966616E4C6900 | CString (length:8) | CrifanLi |
| 00003EB9 | 456172746800 | CString (length:5) | Earth |
| 00003EC2 | 69 | CString (length:0) | |
| 00003EC3 | 6E | CString (length:0) | |
| 00003EC4 | 70 | CString (length:0) | |
| 00003EC5 | 75 | CString (length:0) | |
| 00003EC6 | 74 | CString (length:0) | |
| 00003EC7 | 20 | CString (length:0) | |
| 00003EC8 | 61 | CString (length:0) | |
| 00003EC9 | 72 | CString (length:0) | |
| 00003ECA | 67 | CString (length:0) | |
| 00003ECB | 73 | CString (length:0) | |
| 00003ECC | 3A | CString (length:0) | |
| 00003ECD | 20 | CString (length:0) | |
| 00003ECE | 61 | CString (length:0) | |
| 00003ECF | 72 | CString (length:0) | |
| 00003ED0 | 67 | CString (length:0) | |
| 00003ED1 | 31 | CString (length:0) | |
| 00003ED2 | 5F | CString (length:0) | |
| 00003ED3 | 69 | CString (length:0) | |
| 00003ED4 | 73 | CString (length:0) | |
| 00003ED5 | 43 | CString (length:0) | |
| 00003ED6 | 66 | CString (length:0) | |
| 00003ED7 | 69 | CString (length:0) | |
| 00003ED8 | 6C | CString (length:0) | |
| 00003ED9 | 64 | CString (length:0) | |
| 00003EDA | 3D | CString (length:0) | |
| 00003EDB | 25 | CString (length:0) | |
| 00003EDC | 73 | CString (length:0) | |
| 00003EDD | EF | CString (length:0) | |
| 00003EDE | BC | CString (length:0) | |
| 00003EDF | 8C | CString (length:0) | |
| 00003EE0 | 20617267325F6368696C644167653D25642C206172673... | CString (length:38) | arg2_childAge=%d, arg3_childName=%s\n |
| 00003F06 | 7472756500 | CString (length:4) | true |
| 00003F0B | 66616C736500 | CString (length:5) | false |
| 00003F11 | 6C | CString (length:0) | |
| 00003F12 | 6F | CString (length:0) | |
| 00003F13 | 63 | CString (length:0) | |



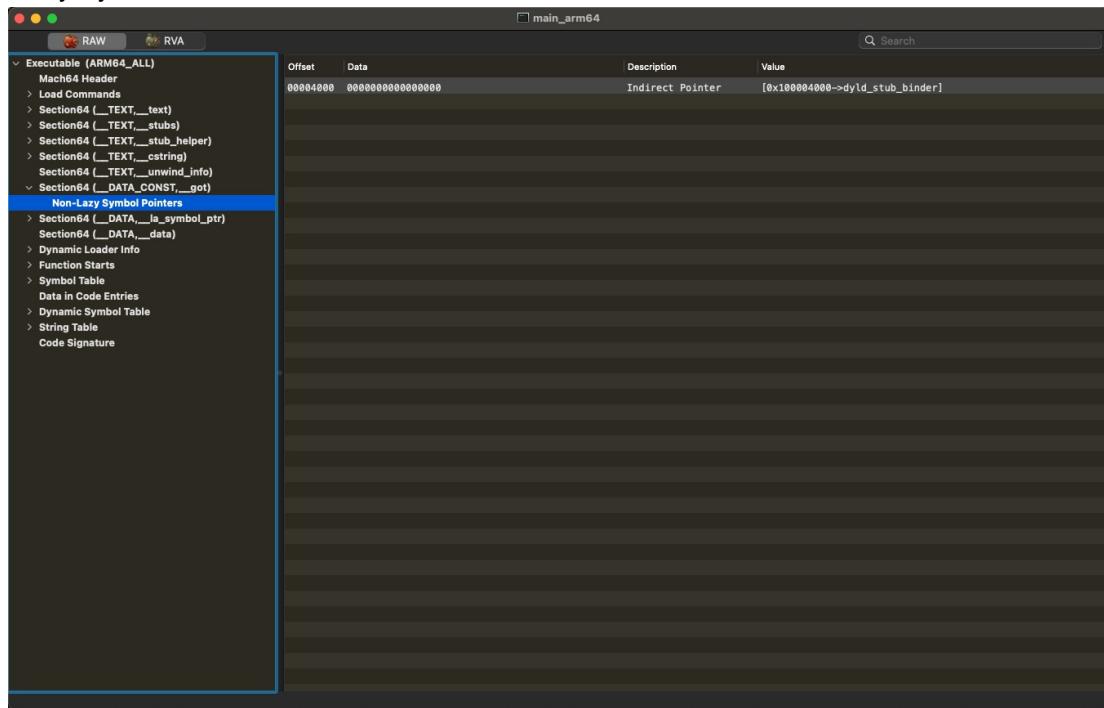
Section64 (__TEXT,__cstring)



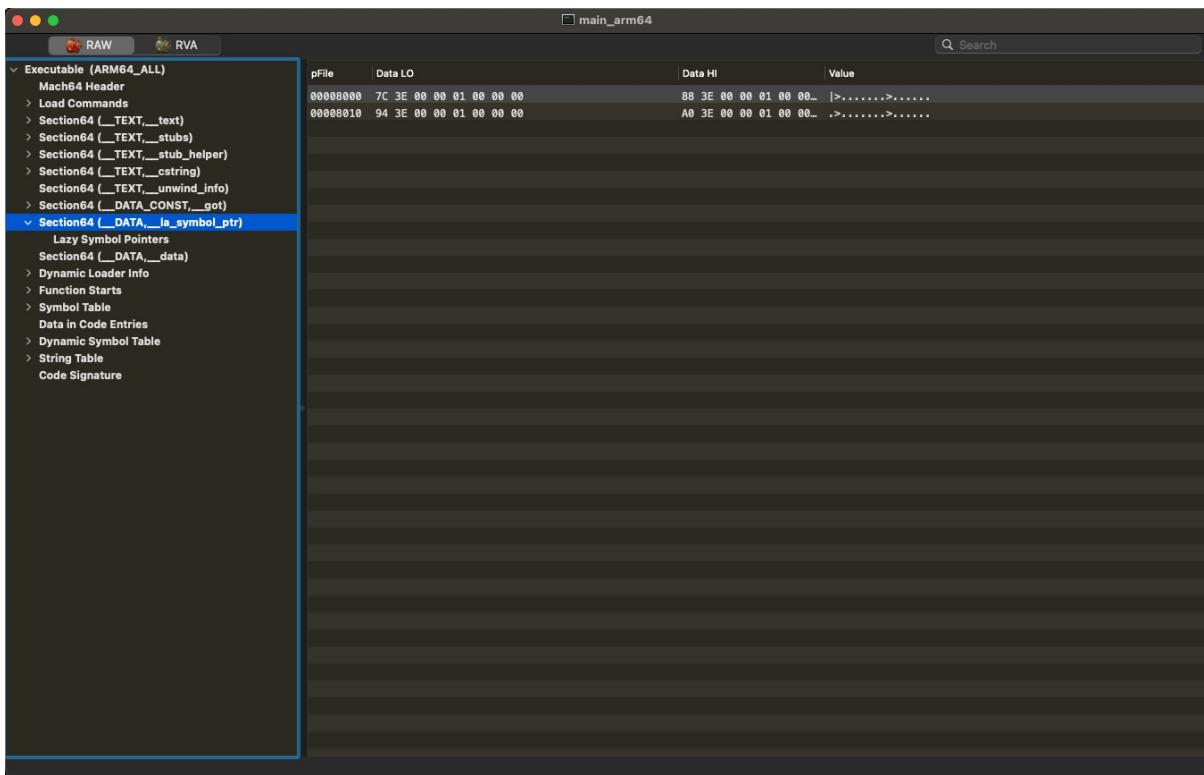
Section64 (__DATA_CONST,__got)



- Non-Lazy Symbol Pointers



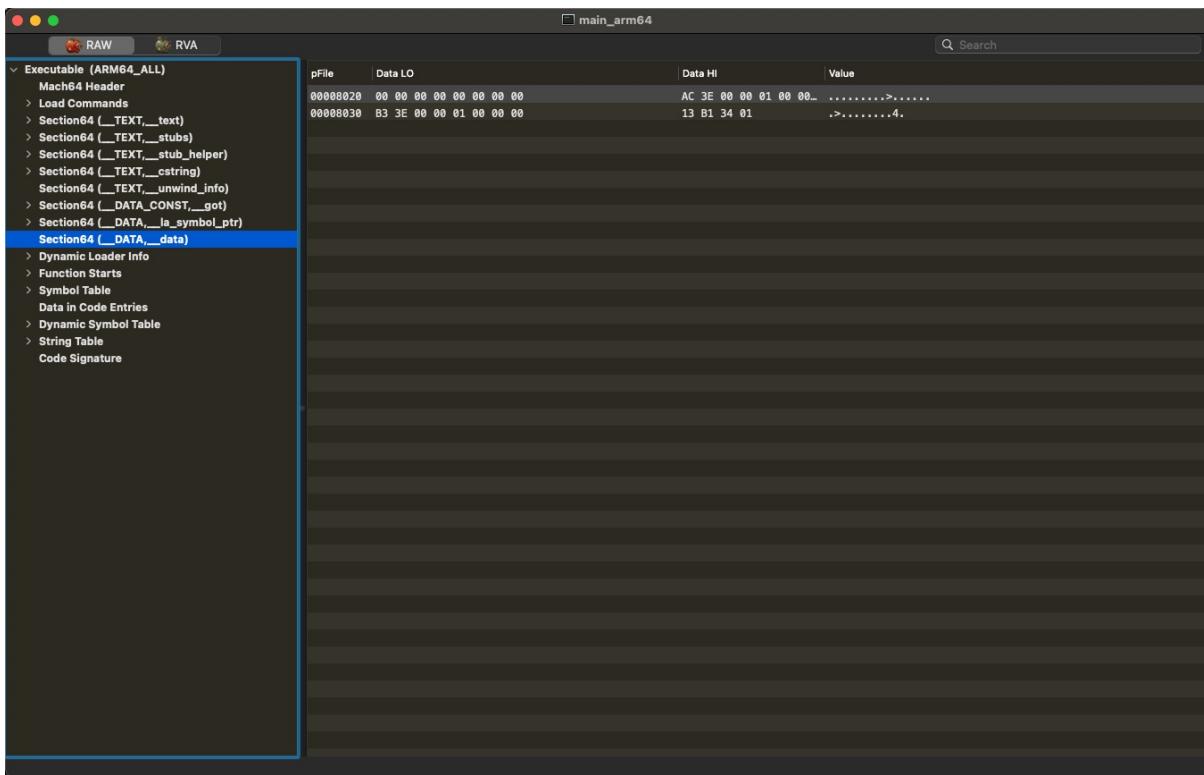
Section64 (__DATA, __la_symbol_ptr)



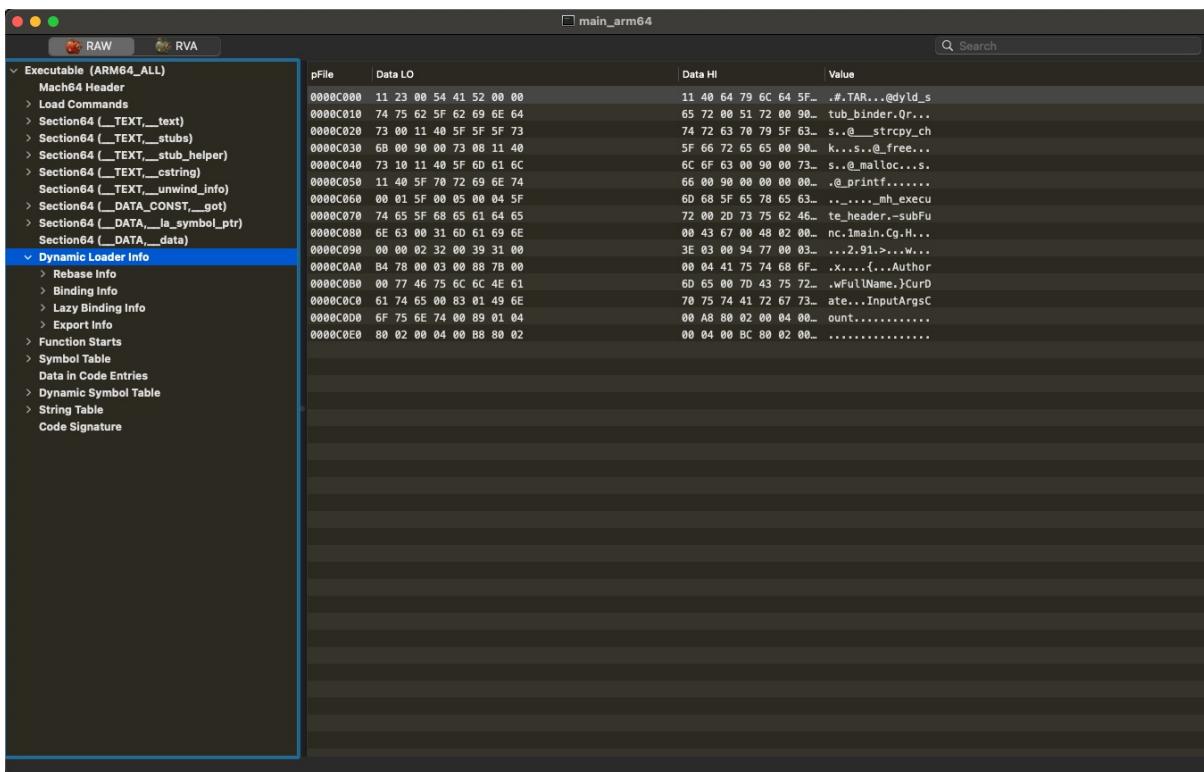
- Lazy Symbol Pointers

| Offset | Data | Description | Value |
|----------|------------------|------------------|---------------------------|
| 00000000 | 0000000100003E7C | Indirect Pointer | [0x10000000->_strcpy_chk] |
| 00000008 | 0000000100003E88 | Indirect Pointer | [0x10000000->_free] |
| 00000010 | 0000000100003E94 | Indirect Pointer | [0x100000010->_malloc] |
| 00000018 | 0000000100003EA0 | Indirect Pointer | [0x100000018->_printf] |

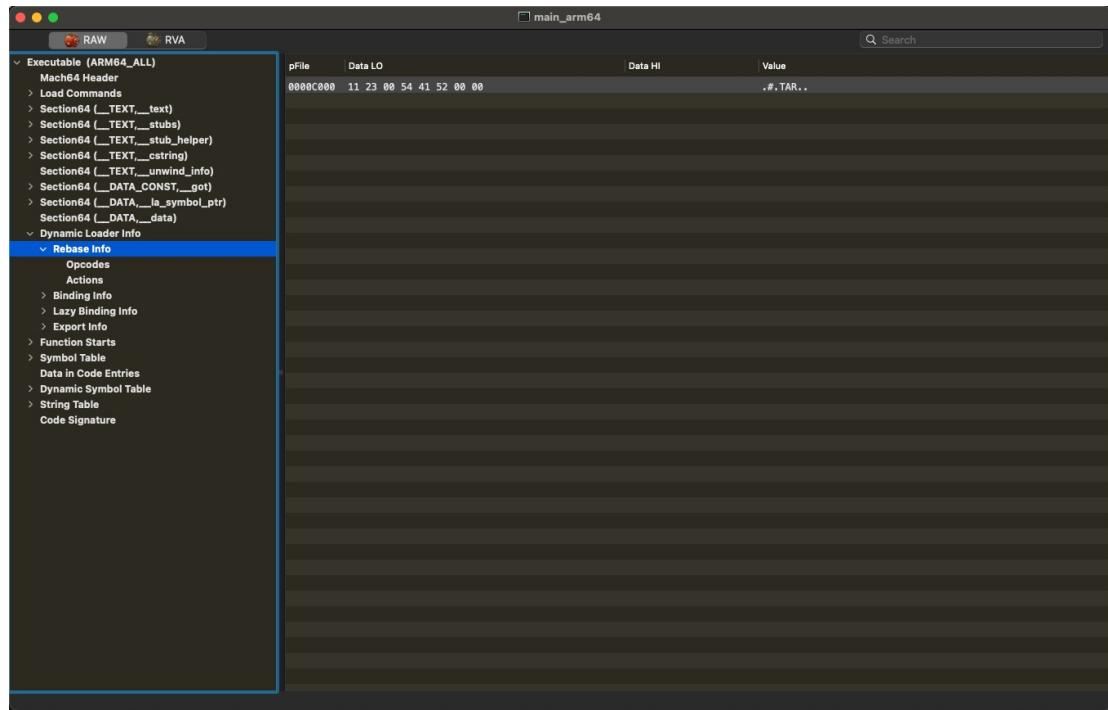
Section64 (__DATA, __data)



Dynamic Loader Info



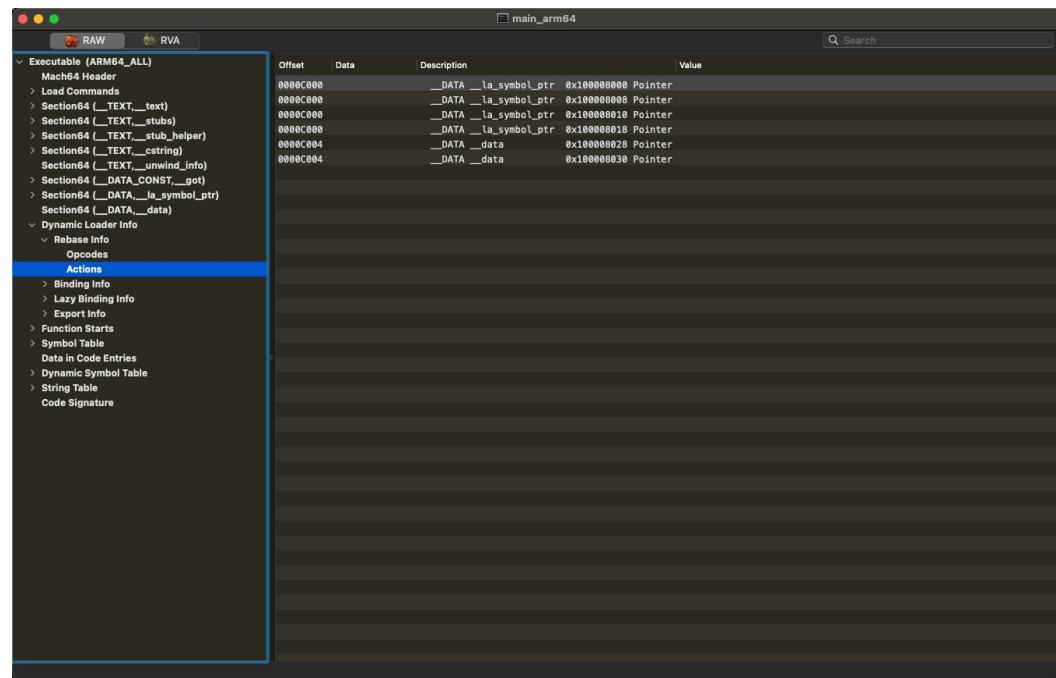
- Rebase Info



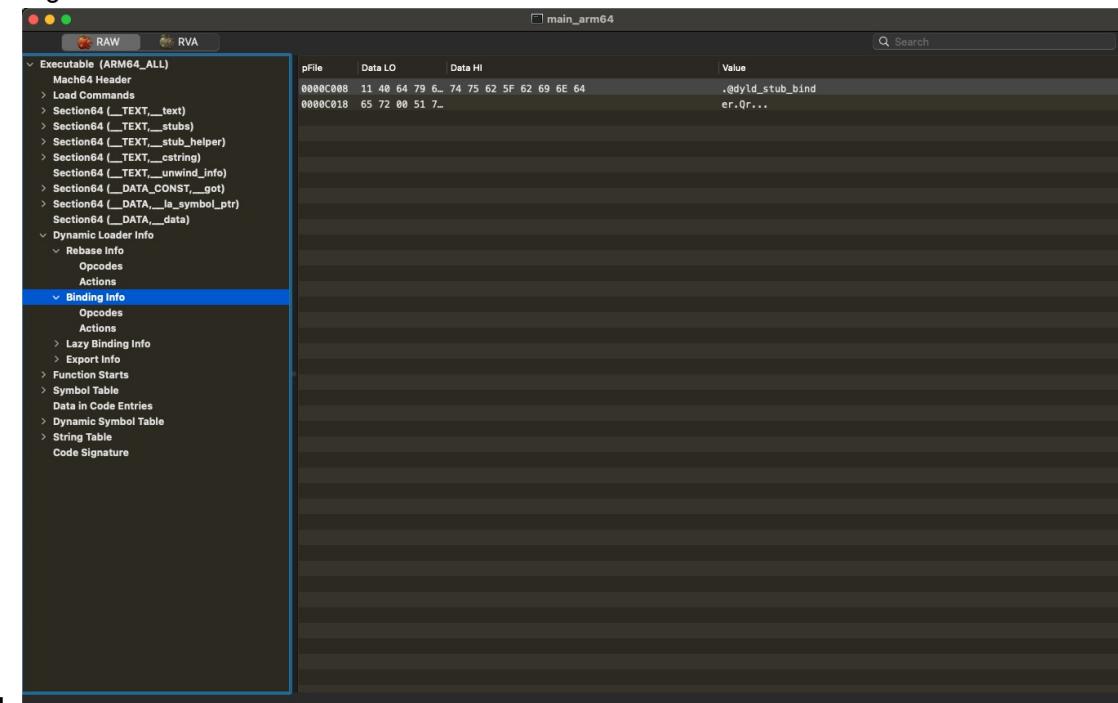
■ Opcodes

| Offset | Data | Description | Value |
|----------|------|---|-------------------------------|
| 0000C000 | 11 | REBASE_OPCODE_SET_TYPE_IMM | type (1, REBASE_TYPE_POINTER) |
| 0000C001 | 23 | REBASE_OPCODE_SET_SEGMENT_AND_OFFSET_ULEB | segment (3) |
| 0000C002 | 00 | uleb128 | offset (8) |
| 0000C003 | 54 | REBASE_OPCODE_DO_REBASE_IMM_TIMES | count (4) |
| 0000C004 | 41 | REBASE_OPCODE_ADD_ADDR_IMM_SCALED | scale (1) |
| 0000C005 | 52 | REBASE_OPCODE_DO_REBASE_IMM_TIMES | count (2) |
| 0000C006 | 00 | REBASE_OPCODE_DONE | |

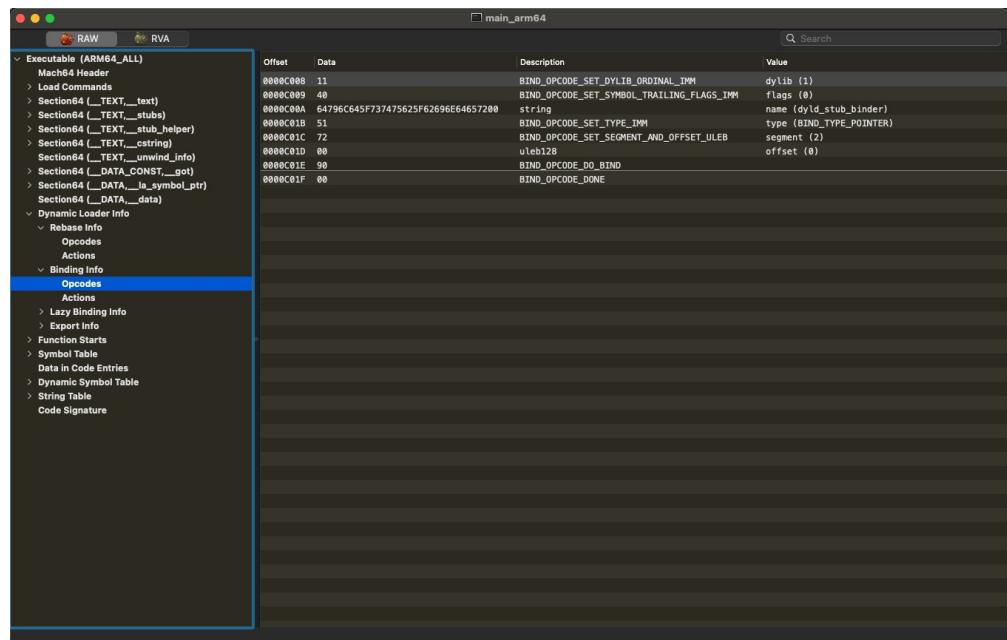
■ Actions



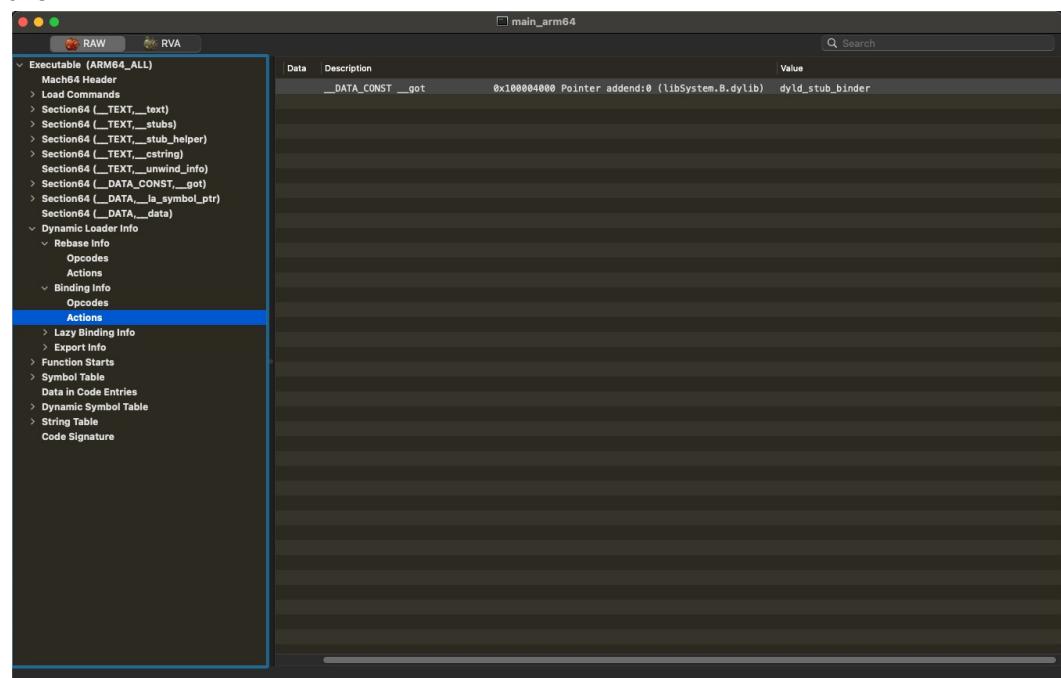
- Binding Info



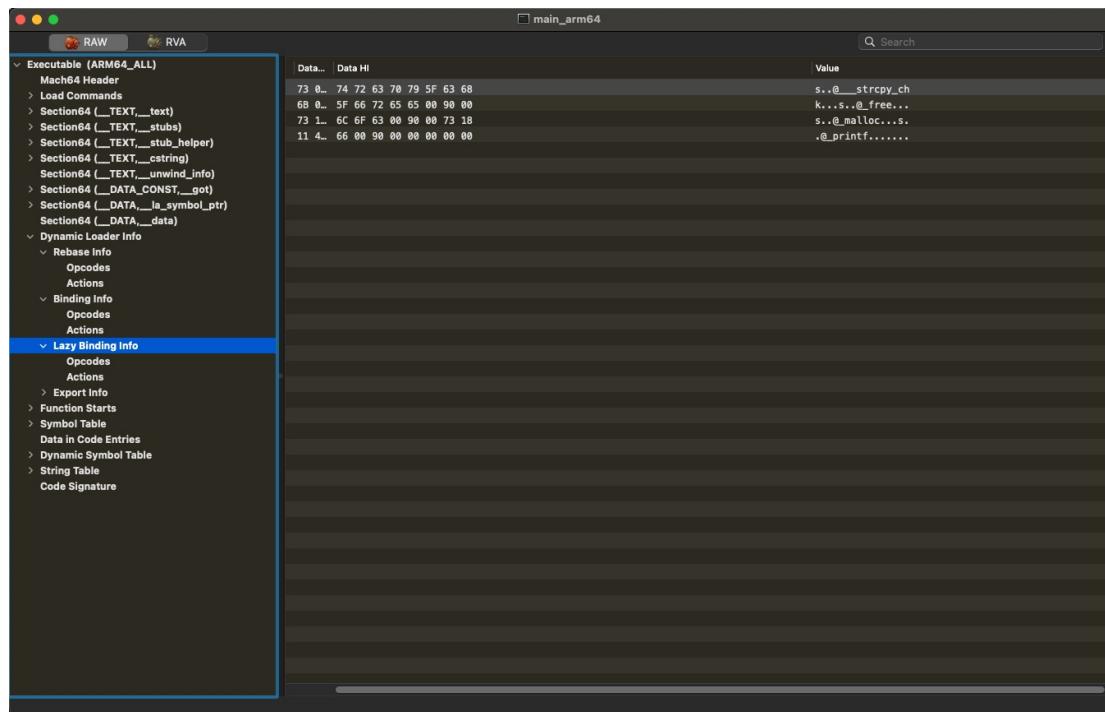
- Opcodes



■ Actions



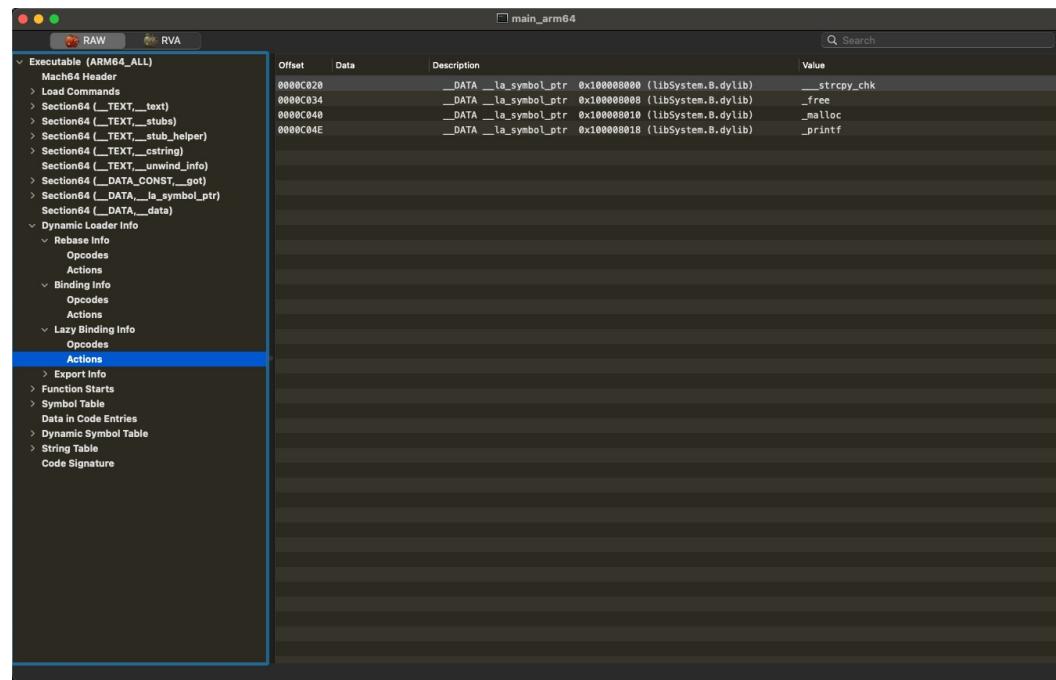
- Lazy Binding Info



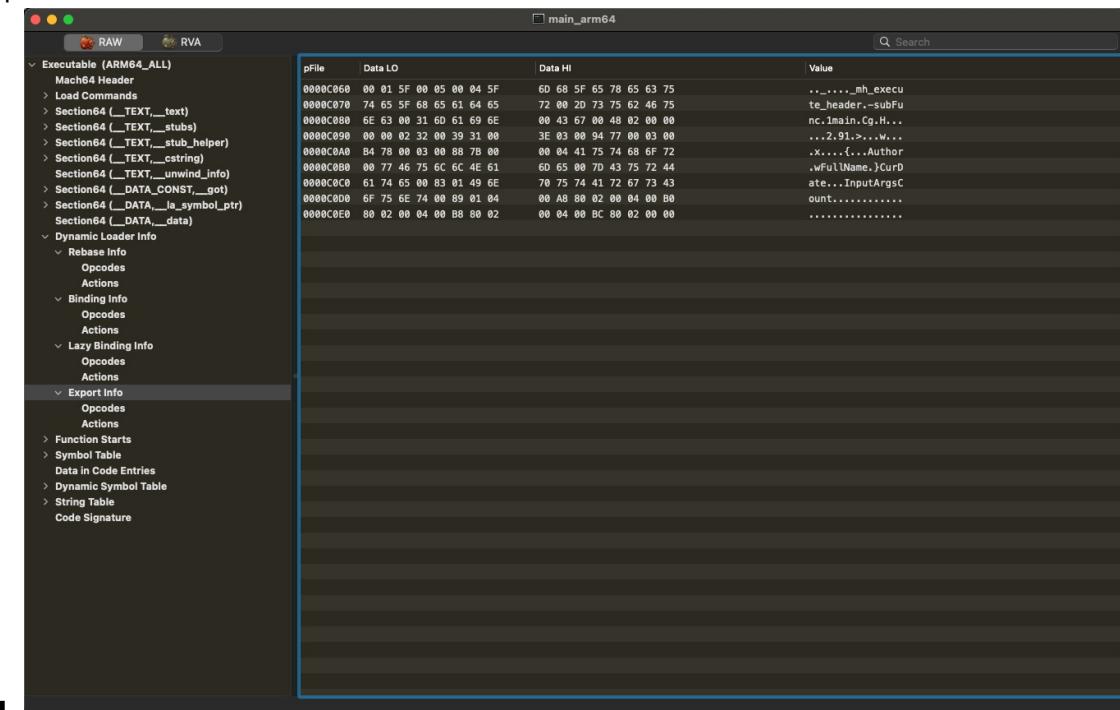
■ Opcodes

| Address | Data | Description | Value |
|---------|-----------------------------|--|---------------------|
| 0xC020 | 73 | BIN_OPCODE_SET_SEGMENT_AND_OFFSET_ULEB | segment (3) |
| 0xC021 | 00 | uleb128 | offset (8) |
| 0xC022 | 11 | BIN_OPCODE_SET_DYLIB_ORDINAL_IMM | dylib (1) |
| 0xC023 | 40 | BIN_OPCODE_SET_SYMBOL_TRAILING_FLAGS_IMM | flags (8) |
| 0xC024 | 5FF5F7374726370795F63686800 | string | name (__strcpy_chk) |
| 0xC032 | 90 | BIN_OPCODE_D0_BIND | |
| 0xC033 | 00 | BIN_OPCODE_DONE | |
| 0xC034 | 73 | BIN_OPCODE_SET_SEGMENT_AND_OFFSET_ULEB | segment (3) |
| 0xC035 | 00 | uleb128 | offset (8) |
| 0xC036 | 11 | BIN_OPCODE_SET_DYLIB_ORDINAL_IMM | dylib (1) |
| 0xC037 | 40 | BIN_OPCODE_SET_SYMBOL_TRAILING_FLAGS_IMM | flags (8) |
| 0xC038 | 5F6672656500 | string | name (_free) |
| 0xC03E | 90 | BIN_OPCODE_D0_BIND | |
| 0xC03F | 00 | BIN_OPCODE_DONE | |
| 0xC040 | 73 | BIN_OPCODE_SET_SEGMENT_AND_OFFSET_ULEB | segment (3) |
| 0xC041 | 10 | uleb128 | offset (16) |
| 0xC042 | 11 | BIN_OPCODE_SET_DYLIB_ORDINAL_IMM | dylib (1) |
| 0xC043 | 40 | BIN_OPCODE_SET_SYMBOL_TRAILING_FLAGS_IMM | flags (8) |
| 0xC044 | 5F60616C6C6F6300 | string | name (_malloc) |
| 0xC04C | 90 | BIN_OPCODE_D0_BIND | |
| 0xC04D | 00 | BIN_OPCODE_DONE | |
| 0xC04E | 73 | BIN_OPCODE_SET_SEGMENT_AND_OFFSET_ULEB | segment (3) |
| 0xC04F | 18 | uleb128 | offset (24) |
| 0xC050 | 11 | BIN_OPCODE_SET_DYLIB_ORDINAL_IMM | dylib (1) |
| 0xC051 | 40 | BIN_OPCODE_SET_SYMBOL_TRAILING_FLAGS_IMM | flags (8) |
| 0xC052 | 5F7072696E746600 | string | name (_printf) |
| 0xC05A | 90 | BIN_OPCODE_D0_BIND | |
| 0xC05B | 00 | BIN_OPCODE_DONE | |
| 0xC05C | 00 | BIN_OPCODE_DONE | |
| 0xC05D | 00 | BIN_OPCODE_DONE | |
| 0xC05E | 00 | BIN_OPCODE_DONE | |
| 0xC05F | 00 | BIN_OPCODE_DONE | |

■ Actions



- Export Info



- Opcodes

Two screenshots of the Immunity Debugger interface showing the symbol table for the main_arm64 executable.

The left screenshot shows the symbol table for the 'Opcodes' section. The right screenshot shows the symbol table for the 'Actions' section.

Symbol Table Headers:

- main_arm64:** Shows the symbol table for the main executable.
- main_arm64:** Shows the symbol table for the main executable.

Symbol Table Columns:

| Offset | Data | Description | Value |
|---|---------------|----------------------|-------|
| 0000C050 00 | Terminal Size | 0 | |
| 0000C051 01 | Child Count | 1 | |
| 0000C052 5F00 | Node Label | " " | |
| 0000C054 05 | Next Node | 0x10000C065 | |
| 0000C055 00 | Terminal Size | 0 | |
| 0000C056 04 | Child Count | 4 | |
| 0000C057 5F6D685F657865637574655F68656164657200 | Node Label | "_mh_execute_header" | |
| 0000C058 00 | Next Node | 0x10000C08D | |
| 0000C059 73756246756E6300 | Node Label | "subFunc" | |
| 0000C05A 00 | Next Node | 0x10000C091 | |
| 0000C05B 6061696E00 | Node Label | "main" | |
| 0000C05C 43 | Next Node | 0x10000C0A3 | |
| 0000C05D 6700 | Node Label | "g" | |
| 0000C05E 48 | Next Node | 0x10000C0A8 | |
| 0000C05F 02 | Terminal Size | 2 | |
| 0000C060 00 | Flags | 00 | |
| 0000C061 00 | Symbol Offset | 0x0 | |
| 0000C062 00 | Child Count | 0 | |
| 0000C063 00 | Terminal Size | 0 | |
| 0000C064 00 | Child Count | 2 | |
| 0000C065 3200 | Node Label | "?" | |
| 0000C066 00 | Next Node | 0x10000C099 | |
| 0000C067 00 | Node Label | "?" | |
| 0000C068 3F | Next Node | 0x10000C09E | |
| 0000C069 03 | Terminal Size | 3 | |
| 0000C06A 00 | Flags | 00 | |
| 0000C06B 9477 | Symbol Offset | 0x3894 | |
| 0000C06C 00 | Child Count | 0 | |
| 0000C06D 00 | Terminal Size | 3 | |
| 0000C06E 00 | Flags | 00 | |
| 0000C06F 00 | Symbol Offset | 0x3D88 | |
| 0000C070 8478 | Child Count | 0 | |
| 0000C071 00 | Terminal Size | 3 | |
| 0000C072 00 | Flags | 00 | |
| 0000C073 8301 | Symbol Offset | 0x3C34 | |
| 0000C074 00 | Child Count | 0 | |
| 0000C075 8901 | Terminal Size | 3 | |
| 0000C076 00 | Flags | 00 | |
| 0000C077 417574686F7200 | Symbol Offset | 0x3D88 | |
| 0000C078 00 | Child Count | 0 | |
| 0000C079 00 | Terminal Size | 0 | |
| 0000C07A 00 | Flags | 00 | |
| 0000C07B 77 | Node Label | "Author" | |
| 0000C07C 00 | Next Node | 0x10000C0D7 | |
| 0000C07D 46756C6C4E616D6500 | Node Label | "FullName" | |
| 0000C07E 7D | Next Node | 0x10000C0D0 | |
| 0000C07F 4375724461746500 | Node Label | "CurDate" | |
| 0000C080 00 | Next Node | 0x10000C0E3 | |
| 0000C081 496E70757441726773436F756E7400 | Node Label | "InputArgsCount" | |
| 0000C082 00 | Next Node | 0x10000C0E9 | |
| 0000C083 00 | Terminal Size | 4 | |
| 0000C084 00 | Flags | 00 | |
| 0000C085 00 | Symbol Offset | 0x8028 | |
| 0000C086 00 | Child Count | 0 | |
| 0000C087 00 | Terminal Size | 4 | |
| 0000C088 00 | Flags | 00 | |
| 0000C089 A88002 | Symbol Offset | 0x8030 | |
| 0000C08A 00 | Child Count | 0 | |
| 0000C08B 00 | Terminal Size | 4 | |
| 0000C08C 00 | Flags | 00 | |
| 0000C08D 00 | Symbol Offset | 0x8032 | |
| 0000C08E 00 | Child Count | 0 | |
| 0000C08F 00 | Terminal Size | 4 | |
| 0000C090 00 | Flags | 00 | |
| 0000C091 00 | Symbol Offset | 0x8034 | |
| 0000C092 00 | Child Count | 0 | |
| 0000C093 00 | Terminal Size | 4 | |
| 0000C094 00 | Flags | 00 | |
| 0000C095 39 | Node Label | "?" | |
| 0000C096 3100 | Next Node | 0x10000C099 | |
| 0000C097 00 | Node Label | "?" | |
| 0000C098 00 | Next Node | 0x10000C09E | |
| 0000C099 03 | Terminal Size | 3 | |
| 0000C09A 00 | Flags | 00 | |
| 0000C09B 9477 | Symbol Offset | 0x3894 | |
| 0000C09C 00 | Child Count | 0 | |
| 0000C09D 00 | Terminal Size | 3 | |
| 0000C09E 03 | Flags | 00 | |
| 0000C09F 00 | Symbol Offset | 0x3D88 | |
| 0000C0A0 8478 | Child Count | 0 | |
| 0000C0A1 00 | Terminal Size | 3 | |
| 0000C0A2 00 | Flags | 00 | |
| 0000C0A3 03 | Node Label | "?" | |
| 0000C0A4 00 | Next Node | 0x10000C0A5 | |
| 0000C0A5 8878 | Node Label | "?" | |
| 0000C0A6 00 | Next Node | 0x10000C0A7 | |
| 0000C0A7 00 | Child Count | 0 | |
| 0000C0A8 00 | Terminal Size | 0 | |
| 0000C0A9 04 | Flags | 00 | |
| 0000C0AA 417574686F7200 | Node Label | "Author" | |
| 0000C0AB 77 | Next Node | 0x10000C0B7 | |
| 0000C0AC 46756C6C4E616D6500 | Node Label | "FullName" | |
| 0000C0AD 7D | Next Node | 0x10000C0D0 | |
| 0000C0AE 4375724461746500 | Node Label | "CurDate" | |
| 0000C0AF 8301 | Next Node | 0x10000C0E3 | |
| 0000C0B0 496E70757441726773436F756E7400 | Node Label | "InputArgsCount" | |
| 0000C0B1 8901 | Next Node | 0x10000C0E9 | |
| 0000C0B2 00 | Terminal Size | 4 | |
| 0000C0B3 00 | Flags | 00 | |
| 0000C0B4 00 | Symbol Offset | 0x8028 | |
| 0000C0B5 00 | Child Count | 0 | |
| 0000C0B6 00 | Terminal Size | 4 | |
| 0000C0B7 00 | Flags | 00 | |
| 0000C0B8 00 | Symbol Offset | 0x8030 | |
| 0000C0B9 00 | Child Count | 0 | |
| 0000C0BA 00 | Terminal Size | 4 | |
| 0000C0BB 00 | Flags | 00 | |
| 0000C0BC 00 | Symbol Offset | 0x8032 | |
| 0000C0BD 00 | Child Count | 0 | |
| 0000C0BE 00 | Terminal Size | 4 | |
| 0000C0BF 00 | Flags | 00 | |
| 0000C0C0 00 | Symbol Offset | 0x8034 | |
| 0000C0C1 00 | Child Count | 0 | |
| 0000C0C2 00 | Terminal Size | 4 | |
| 0000C0C3 00 | Flags | 00 | |
| 0000C0C4 00 | Symbol Offset | 0x8036 | |
| 0000C0C5 00 | Child Count | 0 | |
| 0000C0C6 00 | Terminal Size | 4 | |
| 0000C0C7 00 | Flags | 00 | |
| 0000C0C8 00 | Symbol Offset | 0x8038 | |
| 0000C0C9 00 | Child Count | 0 | |
| 0000C0CA 00 | Terminal Size | 4 | |
| 0000C0CB 00 | Flags | 00 | |
| 0000C0CC 00 | Symbol Offset | 0x803A | |
| 0000C0CD 00 | Child Count | 0 | |
| 0000C0CE 00 | Terminal Size | 4 | |
| 0000C0CF 00 | Flags | 00 | |
| 0000C0D0 00 | Symbol Offset | 0x803C | |
| 0000C0D1 00 | Child Count | 0 | |

■ Actions

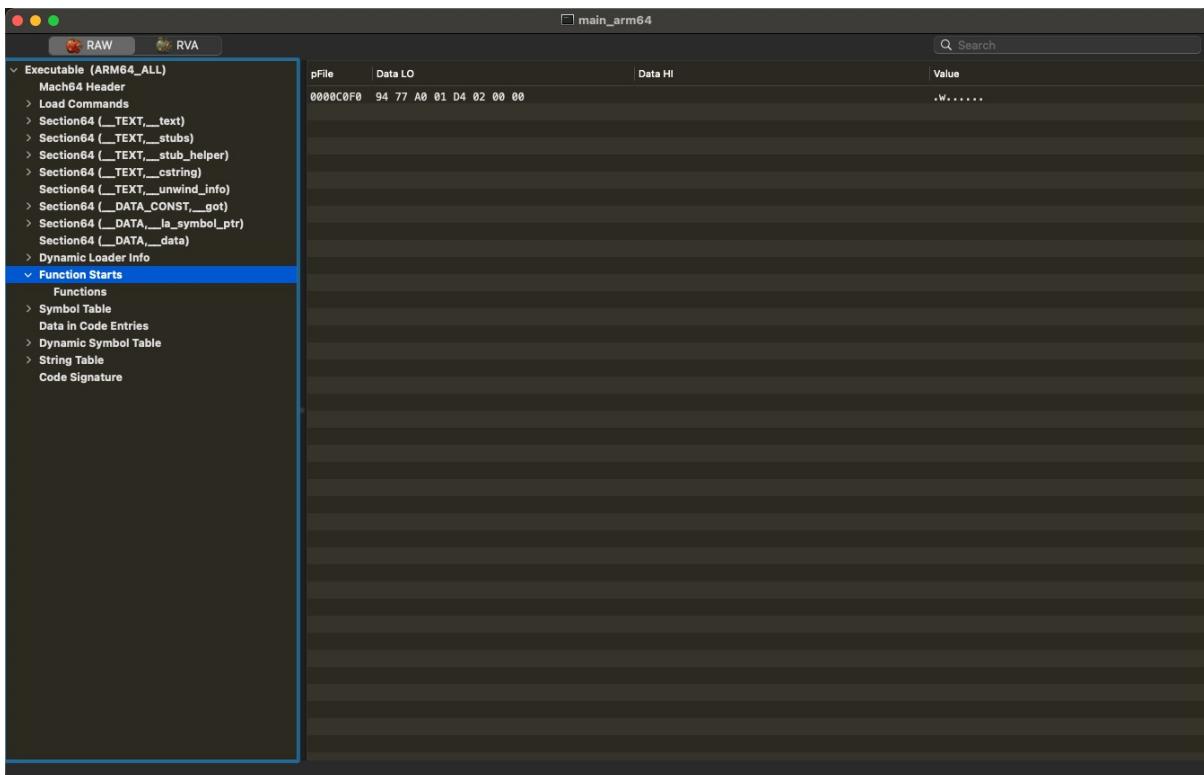
| | Offset | Data | Description | Value |
|--|----------|-----------------|--------------|--------------------|
| | 0000C057 | NO SECTION | 0x1000000000 | _mh_execute_header |
| | 0000C084 | __TEXT __text | 0x100003088 | _main |
| | 0000C093 | __TEXT __text | 0x100003094 | _subfunc2 |
| | 0000C096 | __TEXT __text | 0x100003C34 | _subfunc1 |
| | 0000C0AA | __DATA __data | 0x100000028 | _gAuthor |
| | 0000C0B2 | __DATA __data | 0x100000030 | _gFullName |
| | 0000C0BC | __DATA __data | 0x100000038 | _gCurDate |
| | 0000C0C6 | __DATA __common | 0x10000003C | _gInputArgsCount |

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？

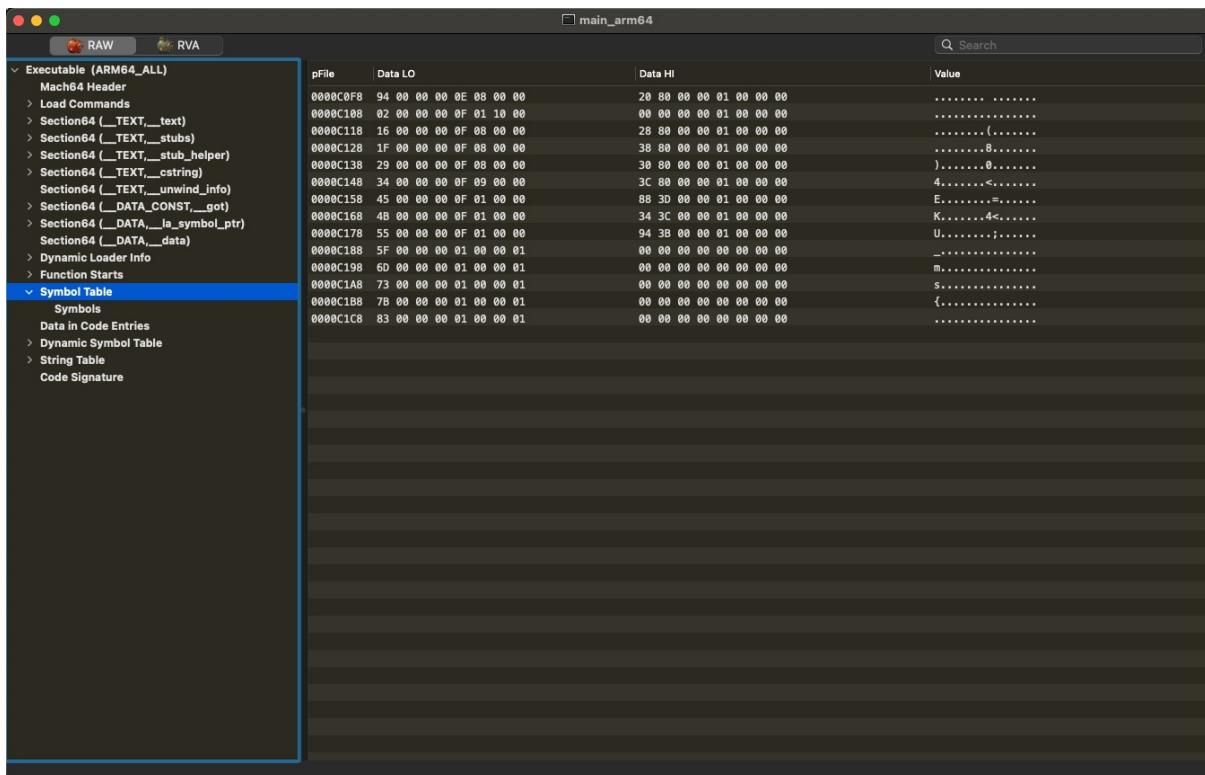
Function Starts



- Functions

| Offset | Data | Description | Value |
|----------|------|-------------|-------------------------|
| 0000C0F0 | 9477 | uleb128 | 0x100003B94 (_subFunc2) |
| 0000C0F2 | A001 | uleb128 | 0x100003C34 (_subFunc1) |
| 0000C0F4 | D402 | uleb128 | 0x100003D88 (_main) |
| 0000C0F6 | 00 | uleb128 | 0x100003D88 (_main) |
| 0000C0F7 | 00 | uleb128 | 0x100003D88 (_main) |

Symbol Table



- Symbols

| Offset | Data | Description | Value |
|----------|------------------|--------------------------|--------------------------------------|
| #0 | | | |
| 0000C0F8 | 00000094 | String Table Index ,#148 | _dyld_private |
| 0000C0FC | 0E | Type | N_SECT |
| 0000C0FD | 08 | Section Index | 8 (_DATA,_data) |
| 0000C0FE | 0000 | Description | |
| 0000C100 | 0000000100000020 | Value | 4295000096 (\$+0) |
| #1 | | | |
| 0000C108 | 00000002 | String Table Index ,#2 | _mh_execute_header |
| 0000C10C | 0F | Type | N_SECT |
| 0000C10D | 01 | Section Index | 1 (_TEXT,_text) |
| 0000C10E | 0010 | Description | REFERENCED_DYNAMICALLY |
| 0000C110 | 0000000100000000 | Value | 4294967296 (\$+18446744073709536364) |
| #2 | | | |
| 0000C118 | 00000016 | String Table Index ,#22 | _gAuthor |
| 0000C11C | 0F | Type | N_SECT |
| 0000C11D | 08 | Section Index | 8 (_DATA,_data) |
| 0000C11E | 0000 | Description | |
| 0000C120 | 0000000100000028 | Value | 4295000104 (\$+8) |
| #3 | | | |
| 0000C128 | 0000001F | String Table Index ,#31 | _gCurDate |
| 0000C12C | 0F | Type | N_SECT |
| 0000C12D | 08 | Section Index | 8 (_DATA,_data) |
| 0000C12E | 0000 | Description | |
| 0000C130 | 0000000100000038 | Value | 4295000120 (\$+24) |
| #4 | | | |
| 0000C138 | 00000029 | String Table Index ,#41 | _gFullName |
| 0000C13C | 0F | Type | N_SECT |
| 0000C13D | 08 | Section Index | 8 (_DATA,_data) |
| 0000C13E | 0000 | Description | |

main_arm64

| Offset | Data | Description | Value |
|---------------------------|--------------------------|-----------------------|-------|
| 0000C128 0000001F | String Table Index ,#31 | _gCurDate | |
| 0000C12C 0F | Type | N_SECT | |
| 0000C12D 0E | 0E | 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 | N_SECT | |
| 0000C13D 0E | 0E | 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 | N_SECT | |
| 0000C14D 0E | 0E | 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 | N_SECT | |
| 0000C15D 0E | 0E | 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 | N_SECT | |
| 0000C16D 0E | 0E | 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 | N_SECT | |
| 0000C17D 0E | 0E | 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 | N_UNDF | |
| 0000C18D 00 | 00 | N_EXT | |
| 0000C18D 00 | Section Index | NO_SECT | |
| 0000C18E 0100 | Description | | |
| 0000C190 0000000000000000 | Library Ordinal | 1 (libSystem.B.dylib) | |
| 0000C190 0000000000000000 | 0100 | N_SYMBOL_RESOLVER | |
| 0000C190 0000000000000000 | Value | 0 | |
| #10 | | | |
| 0000C198 0000006D | String Table Index ,#109 | _free | |
| 0000C19C 01 | Type | N_UNDF | |
| 0000C19D 00 | 00 | N_EXT | |
| 0000C19D 00 | Section Index | NO_SECT | |
| 0000C19E 0100 | Description | | |
| 0000C1A0 0000000000000000 | Library Ordinal | 1 (libSystem.B.dylib) | |
| 0000C1A0 0000000000000000 | 0100 | N_SYMBOL_RESOLVER | |
| 0000C1A0 0000000000000000 | Value | 0 | |
| #11 | | | |
| 0000C1A8 00000073 | String Table Index ,#115 | _malloc | |

Screenshot of the Binary Ninja debugger showing the Symbol Table. The 'Symbols' section is selected in the left sidebar.

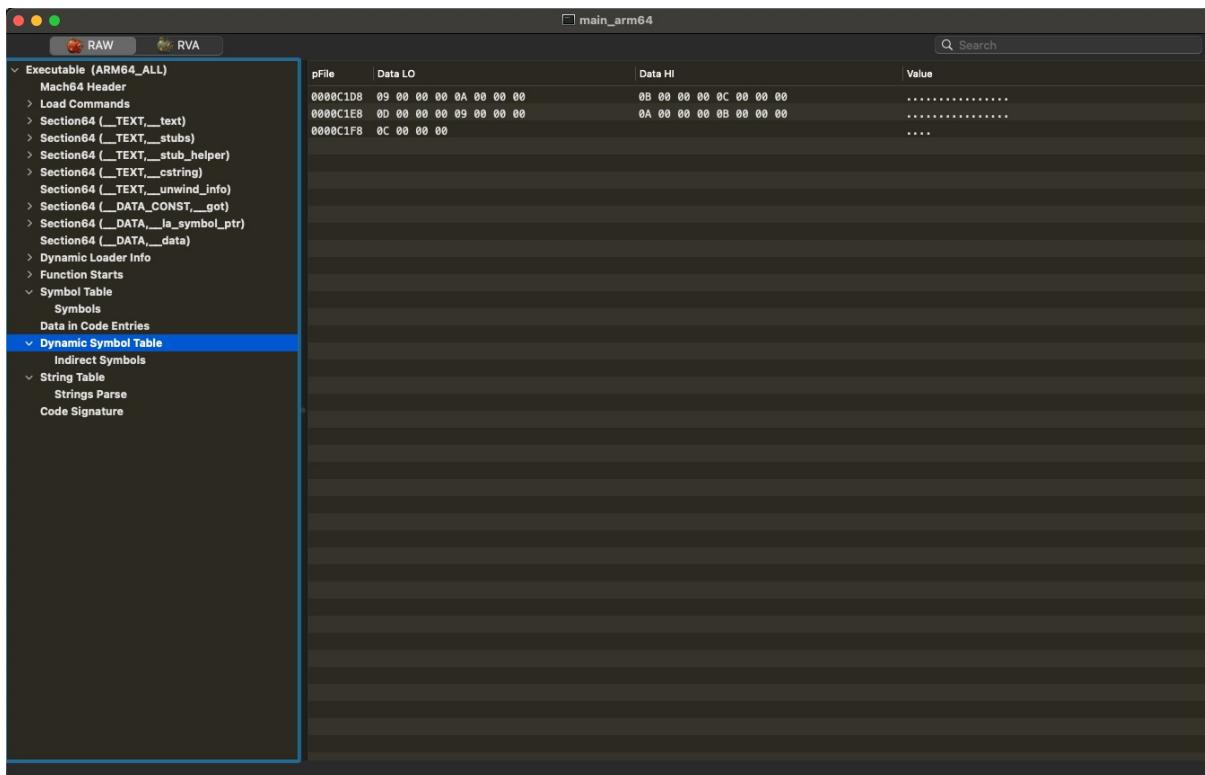
| Offset | Data | Description | Value |
|---------------------------|--------------------------|-----------------------------------|-----------------------|
| 0000C19D 00 | Section Index | N_SECT | |
| 0000C19E 0100 | Description | | |
| | 0 | REFERENCE_FLAG_UNDEFINED_NON_LAZY | |
| | 0100 | Library Ordinal | 1 (libSystem.B.dylib) |
| | 0100 | Section Index | N_SYMBOL_RESOLVER |
| 0000C1A0 0000000000000000 | Description | | 0 |
| #11 | String Table Index ,#115 | _malloc | |
| 0000C1A8 00000073 | Type | | |
| 0000C1AC 01 | 00 | N_UNDEF | |
| | 01 | N_EXT | |
| 0000C1AD 00 | Section Index | N_SECT | |
| 0000C1AE 0100 | Description | | |
| | 0 | REFERENCE_FLAG_UNDEFINED_NON_LAZY | |
| | 0100 | Library Ordinal | 1 (libSystem.B.dylib) |
| | 0100 | Section Index | N_SYMBOL_RESOLVER |
| 0000C1B0 0000000000000000 | Description | | 0 |
| #12 | String Table Index ,#123 | _printf | |
| 0000C1B8 0000007B | Type | | |
| 0000C1BC 01 | 00 | N_UNDEF | |
| | 01 | N_EXT | |
| 0000C1BD 00 | Section Index | N_SECT | |
| 0000C1BE 0100 | Description | | |
| | 0 | REFERENCE_FLAG_UNDEFINED_NON_LAZY | |
| | 0100 | Library Ordinal | 1 (libSystem.B.dylib) |
| | 0100 | Section Index | N_SYMBOL_RESOLVER |
| 0000C1C0 0000000000000000 | Description | | 0 |
| #13 | String Table Index ,#131 | dyld_stub_binder | |
| 0000C1C8 00000083 | Type | | |
| 0000C1CC 01 | 00 | N_UNDEF | |
| | 01 | N_EXT | |
| 0000C1CD 00 | Section Index | N_SECT | |
| 0000C1CE 0100 | Description | | |
| | 0 | REFERENCE_FLAG_UNDEFINED_NON_LAZY | |
| | 0100 | Library Ordinal | 1 (libSystem.B.dylib) |
| | 0100 | Section Index | N_SYMBOL_RESOLVER |
| 0000C1D0 0000000000000000 | Description | | 0 |

Data in Code Entries

Screenshot of the Binary Ninja debugger showing the Data in Code Entries. The 'Data in Code Entries' section is selected in the left sidebar.

| pFile | Data LO | Data HI | Value |
|-------|---------|---------|-------|
| | | | |

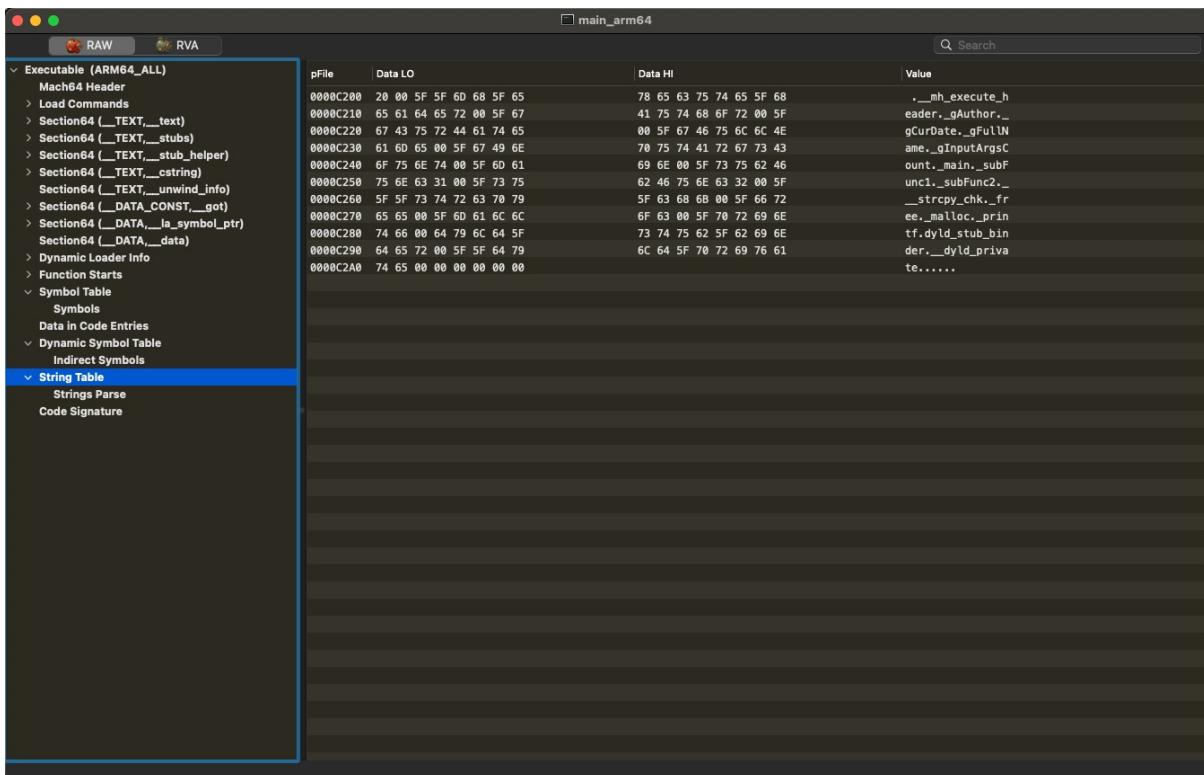
Dynamic Symbol Table



- Indirect Symbols

| Offset | Data | Description | Value |
|--------|-------------------|--|--|
| #0 | 0000C1D8 00000009 | Symbol Table Index ,#9
Section
Indirect Address | __strcpy_chk
(__TEXT,__stubs)
0x100003E34 (\$+0) |
| #1 | 0000C1DC 0000000A | Symbol Table Index ,#10
Section
Indirect Address | _free
(__TEXT,__stubs)
0x100003E40 (\$+12) |
| #2 | 0000C1E0 0000000B | Symbol Table Index ,#11
Section
Indirect Address | _malloc
(__TEXT,__stubs)
0x100003E4C (\$+24) |
| #3 | 0000C1E4 0000000C | Symbol Table Index ,#12
Section
Indirect Address | _printf
(__TEXT,__stubs)
0x100003E58 (\$+36) |
| #4 | 0000C1E8 0000000D | Symbol Table Index ,#13
Section
Indirect Address | dyld_stub_binder
(__DATA_CONST,__got)
0x100004000 (\$+0) |
| #5 | 0000C1EC 00000009 | Symbol Table Index ,#9
Section
Indirect Address | __strcpy_chk
(__DATA,__la_symbol_ptr)
0x100008000 (\$+0) |
| #6 | 0000C1F0 0000000A | Symbol Table Index ,#10
Section
Indirect Address | _free
(__DATA,__la_symbol_ptr)
0x100008008 (\$+8) |
| #7 | 0000C1F4 0000000B | Symbol Table Index ,#11
Section
Indirect Address | _malloc
(__DATA,__la_symbol_ptr)
0x100008010 (\$+16) |
| #8 | 0000C1F8 0000000C | Symbol Table Index ,#12
Section
Indirect Address | _printf
(__DATA,__la_symbol_ptr)
0x100008018 (\$+24) |

String Table



- Strings Parse

| Offset | Data | Description | Value |
|--------|----------|--|---------------------|
| #0 | 0000C200 | 2000 | CString (length:1) |
| #2 | 0000C202 | 5F5F6D685F657865637574655F686561646572 | CString (length:19) |
| #22 | 0000C216 | 5F67417574686F7200 | CString (length:8) |
| #31 | 0000C21F | 5F674375724461746500 | CString (length:9) |
| #41 | 0000C229 | 5F6746756C6C4E616D6500 | CString (length:10) |
| #52 | 0000C234 | 5F67496E70757441726773436F756E7400 | CString (length:16) |
| #59 | 0000C245 | 5F6D61696E00 | CString (length:5) |
| #75 | 0000C24B | 5F73756246756E633100 | CString (length:9) |
| #85 | 0000C255 | 5F73756246756E633200 | CString (length:9) |
| #95 | 0000C25F | 5F5F5F7374726370795F63686800 | CString (length:13) |
| #109 | 0000C260 | 5F6672656500 | CString (length:5) |
| #115 | 0000C273 | 5F6D616C6C6F6300 | CString (length:7) |
| #123 | 0000C27B | 5F7072696E746600 | CString (length:7) |
| #131 | 0000C283 | 64796C645F737475625F62696E64657200 | CString (length:16) |
| #148 | 0000C294 | 5F5F64796C645F7072697661746500 | CString (length:14) |
| #163 | 0000C2A3 | 00 | CString (length:0) |
| #164 | 0000C2A4 | 00 | CString (length:0) |
| #165 | 0000C2A5 | 00 | CString (length:0) |
| #166 | 0000C2A6 | 00 | CString (length:0) |
| #167 | 0000C2A7 | 00 | CString (length:0) |

Code Signature

| Address | Data LO | Data HI | Value |
|----------|----------------------------|----------------------------|-------------------|
| 0000C2B0 | FA DE 0C C0 00 00 00 02 17 | 00 00 00 01 00 00 00 00 00 | |
| 0000C2C0 | 00 00 00 14 FA DE 0C 02 | 00 00 02 03 00 02 04 00 |c..X.. |
| 0000C2D0 | 00 02 00 02 00 00 00 00 63 | 00 00 00 58 00 00 00 00 | |
| 0000C2E0 | 00 00 00 00 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 00 | |
| 0000C300 | 00 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 00 01 60 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 00 4E 6D 8A 9A 65 14 | 17 B5 53 72 09 38 5D 2B | .Nm..e..\$r.8]+ |
| 0000C340 | EF 60 B7 80 38 04 24 AD | 7F AC B2 58 6F C6 E9 66 | .m..8.\$....Xo..f |
| 0000C350 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C360 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C370 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C380 | DA BD 8B 48 89 2C A7 D1 | CA E8 FC 7E 5A 1A 61 37 |H,...~.z.2.7 |
| 0000C390 | 05 EF B2 4F F2 BF E2 AE | 3A 77 39 1C 54 53 B9 32 | ..0....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 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C3C0 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C3D0 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C3E0 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C3F0 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C400 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C410 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C420 | DA BD 8B 48 89 2C A7 42 | 79 BF 5D 54 CC B6 B6 00 |H.,By.lT.... |
| 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 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C460 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C470 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C480 | DA BD 8B 48 89 2C A7 AD | 7F AC B2 58 6F C6 E9 66 |H,...Xo..f |
| 0000C490 | C8 04 07 D1 D1 6B 02 4F | 58 05 FF 7C B4 7C 7A 85 |k.OX..l. z. |
| 0000C4A0 | DA BD 8B 48 89 2C A7 A | 0C 00 8A 06 C9 41 EF 2E |H.,z....A.. |
| 0000C4B0 | 7A 8C 1B 7F 7E 2D 11 46 | BB 24 CD CD 03 85 FB 58 | z....~.F,\$....X |
| 0000C4C0 | D0 A7 9B 13 66 4F 7E | |f0~ |

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 23:12:32

MachOView用法举例：AwemeCore

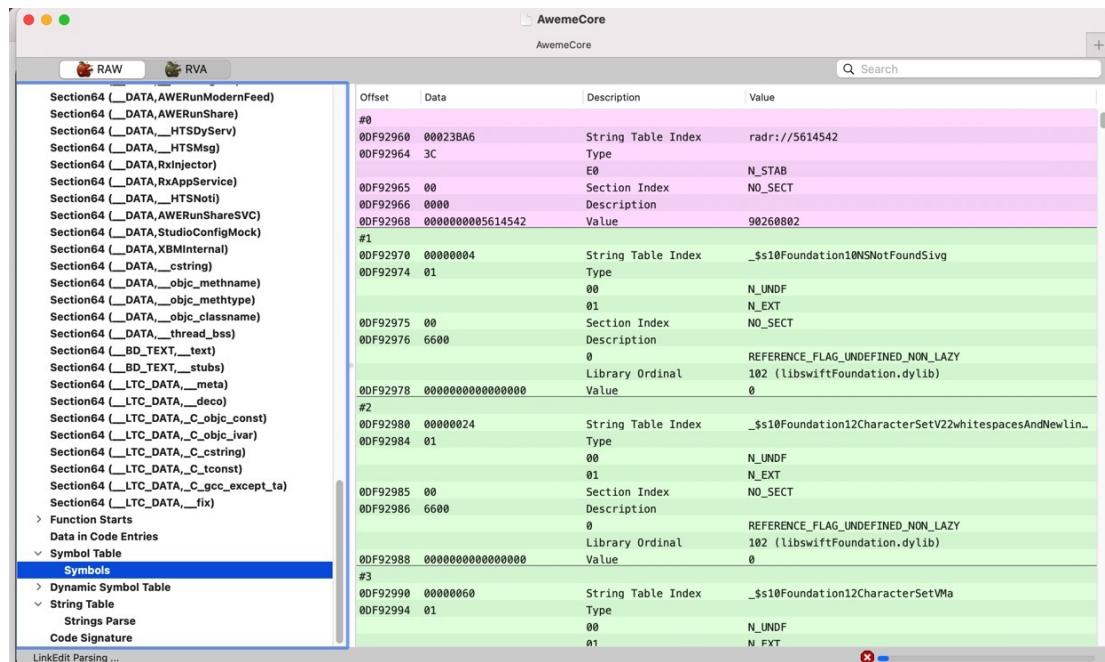
- Mach64 Header

◦

- Symbol Table

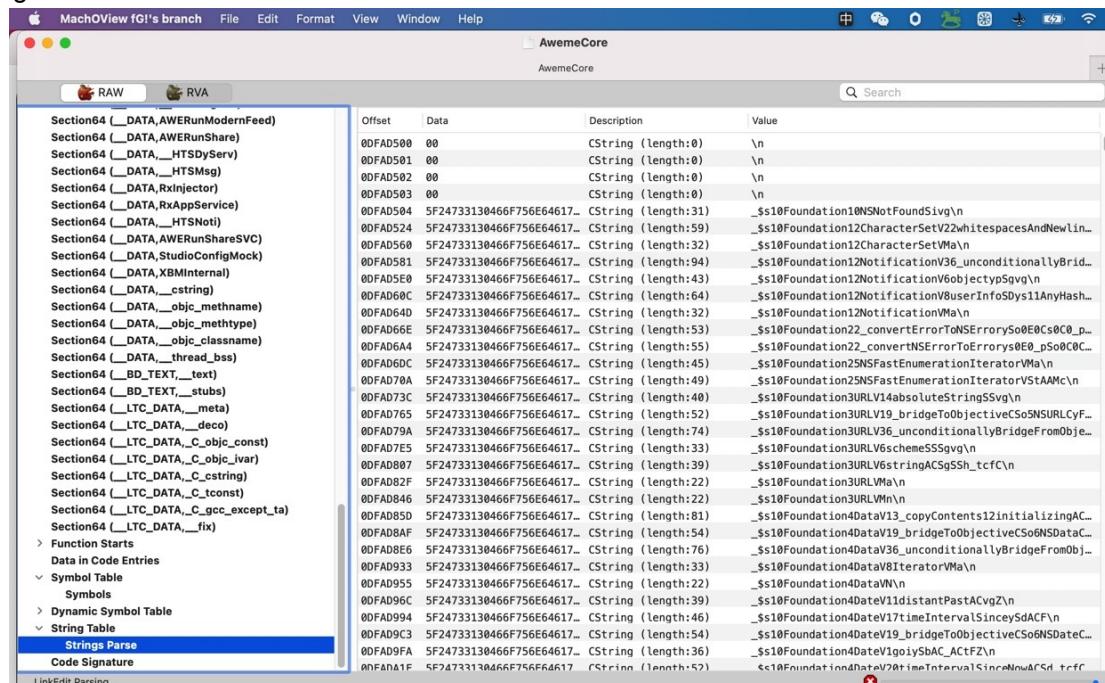
◦

- Symbols



- String Table

- Strings Parse



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

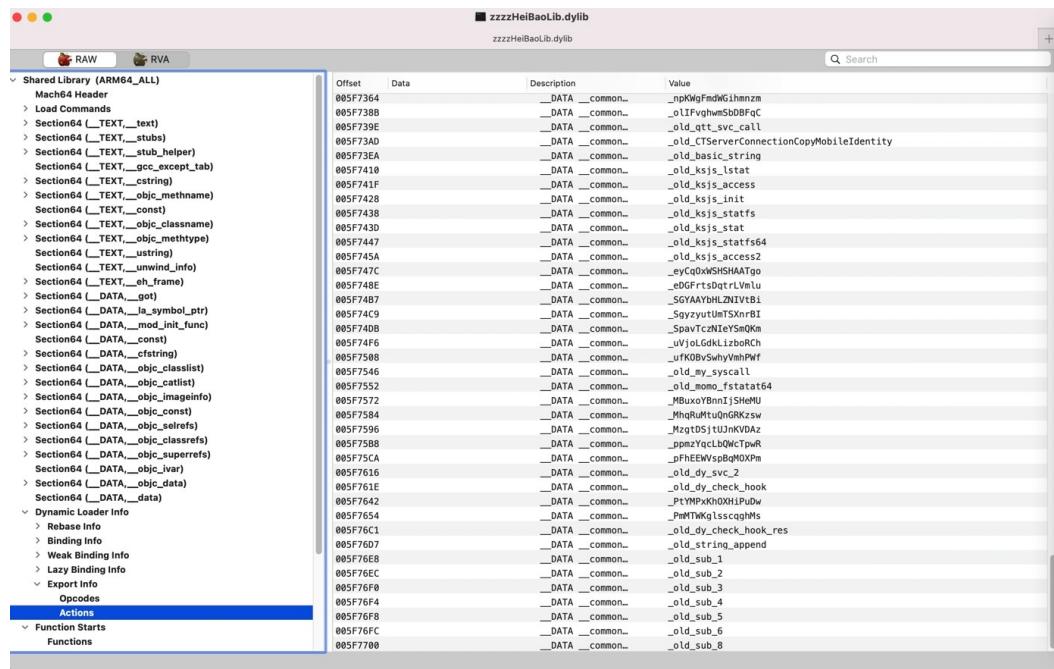
2023-10-07 23:23:00

MachOView用法举例：zzzzHeiBaoLib.dylib

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

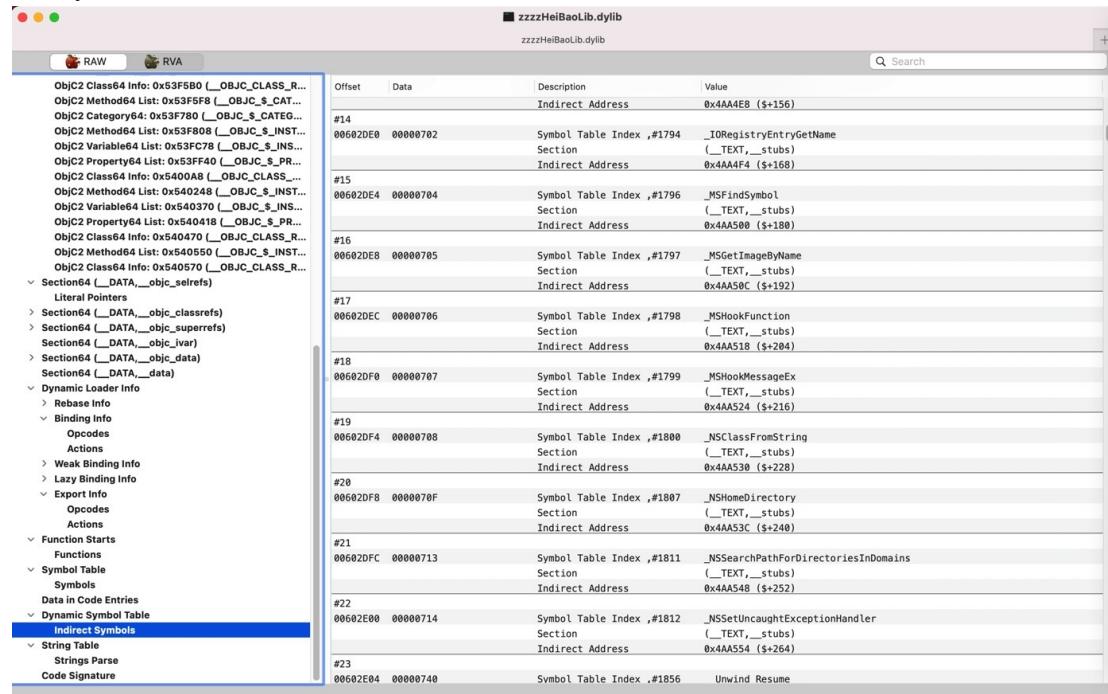
-
- `__TEXT,__objc_methname`

-
- Dynamic Loader Info
 - Export Info
 - Actions



- Dynamic Symbol Table

- Indirect Symbols



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 23:22:35

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:38:26

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:37:07

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](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-04 23:22:41

rabin2用法

- **-I** : File Identification

```
rabin2 -I binaryFile
```

- **-e** : Entrypoint

```
rabin2 -e binaryFile
```

- **-i** : Imports

```
rabin2 -i binaryFile
```

- **-E** : Exports

```
rabin2 -E binaryFile
```

- **-s** : Symbols

```
rabin2 -s binaryFile
```

- **-l** : Libraries

```
rabin2 -l binaryFile
```

- **-z** : Strings

```
rabin2 -z binaryFile
```

- **s** : Program Sections

```
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
```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-05 16:33:26

rabin2用法举例

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-05 16:47:02

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/AwemeCore.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/AwemeCore.framework/AwemeCore
fs symbols
"f entry0 1 0x00023448"
"f entry0_haddr 1 0xffffffffffffffffffff"
"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.In |
| 1 | 0x11476a44 NONE FUNC | sym.imp.static Foundation.CharacterSet.whitespa |
| 2 | 0x11476a50 NONE FUNC | cesAndNewlines.getter ↳ Foundation.CharacterSet |
| 3 | 0x11476a5c NONE FUNC | sym.imp.type metadata accessor for Foundation.C |
| 4 | 0x11476a68 NONE FUNC | haracterSet |
| 5 | 0x11476a74 NONE FUNC | sym.imp.static Foundation.Notification._uncondi |
| 6 | 0x11476a80 NONE FUNC | tionallyBridgeFromObjectiveC(Swift.Optional __C.NSNotification) -> Foundation.Notification |
| 7 | 0x11476a8c NONE FUNC | sym.imp.Foundation.Notification.object.getter ↳ |
| 8 | 0x11476a98 NONE FUNC | Swift.Optional Any |
| 9 | 0x11476aa4 NONE FUNC | sym.imp.Foundation.Notification.userInfo.getter ↳ |
| 10 | 0x00000000 NONE FUNC | Swift.Optional Swift.Dictionary Swift.AnyHashable, Any |
| 11 | 0x11476ab0 NONE FUNC | sym.imp.type metadata accessor for Foundation.N |
| 12 | 0x11476abc NONE FUNC | otification |
| 13 | 0x11476ac8 NONE FUNC | sym.imp.Foundation._convertErrorToNSError(Swift |
| 14 | 0x11476ad4 NONE FUNC | .Error) -> __C.NSError |
| 15 | 0x11476ae0 NONE FUNC | sym.imp.Foundation._convertNSErrorToError(Swift |
| 16 | 0x11476aec NONE FUNC | .Optional __C.NSError) -> Swift.Error |
| 17 | 0x00000000 NONE FUNC | sym.imp.type metadata accessor for Foundation.N |
| 18 | 0x11476af8 NONE FUNC | SFastEnumerationIterator |
| 19 | 0x11476b04 NONE FUNC | sym.imp.protocol conformance descriptor for Fou |
| 20 | 0x11476b10 NONE FUNC | nclusion.NSFastEnumerationIterator ↳ Swift.IteratorProtocol in Foundation |
| 21 | 0x11476b1c NONE FUNC | sym.imp.Foundation.URL.absoluteString.getter ↳ |
| 22 | 0x00000000 NONE FUNC | Swift.String |
| | | sym.imp.Foundation.URL._bridgeToObjectiveC() -> |
| | | __C.NSURL |
| | | sym.imp.static Foundation.URL._unconditionallyB |
| | | ridgeFromObjectiveC(Swift.Optional __C.NSURL) -> Foundation.URL |
| | | sym.imp.Foundation.URL.scheme.getter ↳ Swift.Op |
| | | tional Swift.String |
| | | sym.imp.Foundation.URL.init(string: __shared Sw |
| | | ift.String) -> Swift.Optional Foundation.URL |
| | | sym.imp.type metadata accessor for Foundation.U |
| | | RL |
| | | sym.imp.nominal type descriptor for Foundation. |
| | | URL |
| | | sym.imp.Foundation.Data._copyContents(initializ |
| | | ing: Swift.UnsafeMutableBufferPointer Swift.UInt8) -> (Foundation.Data.Iterator, Swift |
| | | .Int) |
| | | sym.imp.Foundation.Data._bridgeToObjectiveC() -> |
| | | __C.NSDData |
| | | sym.imp.static Foundation.Data._unconditionally |
| | | BridgeFromObjectiveC(Swift.Optional __C.NSDData) -> Foundation.Data |
| | | sym.imp.type metadata accessor for Foundation.D |
| | | ata.Iterator |
| | | sym.imp.type metadata for Foundation.Data |

```

23  0x11476b28 NONE FUNC           sym.imp.static Foundation.Date.distantPast.gett
er + Foundation.Date
24  0x11476b34 NONE FUNC           sym.imp.Foundation.Date.timeIntervalSince(Found
ation.Date) -> Swift.Double
25  0x11476b40 NONE FUNC           sym.imp.Foundation.Date._bridgeToObjectiveC() ->
__C.NSDate
26  0x11476b4c NONE FUNC           sym.imp.static Foundation.Date.> infix(Foundati
on.Date, Foundation.Date) -> Swift.Bool
27  0x11476b58 NONE FUNC           sym.imp.Foundation.Date.init(timeIntervalSinceN
ow: Swift.Double) -> Foundation.Date
28  0x11476b64 NONE FUNC           sym.imp.Foundation.Date.init() -> Foundation.Da
te
29  0x11476b70 NONE FUNC           sym.imp.type metadata accessor for Foundation.D
ate
30  0x00000000 NONE FUNC           sym.imp.nominal type descriptor for Foundation.
Date
31  0x11476b7c NONE FUNC           sym.imp.Foundation.UUID.randomUUID.getter + Swi
ft.String
32  0x11476b88 NONE FUNC           sym.imp.type metadata accessor for Foundation.U
UID
33  0x11476b94 NONE FUNC           sym.imp.FoundationIndexPath._bridgeToObjectiveC
() -> __C.NSIndexPath
34  0x11476ba0 NONE FUNC           sym.imp.static FoundationIndexPath._unconditio
nallyBridgeFromObjectiveC(Swift.Optional __C.NSIndexPath) -> FoundationIndexPath
35  0x11476bac NONE FUNC           sym.imp.(extension in UIKit):FoundationIndexPath
.init(row: Swift.Int, section: Swift.Int) -> FoundationIndexPath
36  0x11476bb8 NONE FUNC           sym.imp.(extension in UIKit):FoundationIndexPath
.row.getter + Swift.Int
37  0x11476bc4 NONE FUNC           sym.imp.(extension in UIKit):FoundationIndexPath
.init(item: Swift.Int, section: Swift.Int) -> FoundationIndexPath
38  0x11476bd0 NONE FUNC           sym.imp.(extension in UIKit):FoundationIndexPath
.item.getter + Swift.Int
39  0x11476bdc NONE FUNC           sym.imp.(extension in UIKit):FoundationIndexPath
.section.getter + Swift.Int
40  0x11476be8 NONE FUNC           sym.imp.type metadata accessor for Foundation.I
ndexPath
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 | wcsncmp |
| 4963 0x1147ec40 NONE FUNC | wcsncpy |
| 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 | 0x1147eee4 | 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 Fou
ndation.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.userInfo
o.getter + Swift.Optional Swift.Dictionary<Swift.AnyHashable, Any>
6 0x11476a80 NONE FUNC           sym.imp.type metadata accessor for Fou
ndation.Notification
7 0x11476a8c NONE FUNC           sym.imp.Foundation._convertErrorToNSError
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 Fou
ndation.NSFastEnumerationIterator

```

- nm

```

U __$s10Foundation10NSNotFoundS4vg
U __$s10Foundation12CharacterSetV22whitespacesAndNewlinesACvgZ
U __$s10Foundation12CharacterSetVMa
U __$s10Foundation12NotificationV36_unconditionallyBridgeFromObjectiveCyACSo14NS
NotificationCSgFZ
U __$s10Foundation12NotificationV6objectypS4vg
U __$s10Foundation12NotificationV8userInfoSDys11AnyHashableVypGSgvg
U __$s10Foundation12NotificationVMa
U __$s10Foundation22_convertErrorToNSErrorySo0E0Cs0C0_pF
U __$s10Foundation22_convertNSErrorToErrorrys0E0_pSo0C0CSgF
U __$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 + Swift.t.Int |
| 2 | 0x0cad6a44 | 0x11476a44 | LOCAL | FUNC 0 | | static Foundation.CharacterSet.whitespaceAndNewlines.getter + Foundation.CharacterSet |
| 3 | 0x0cad6a50 | 0x11476a50 | LOCAL | FUNC 0 | | type metadata accessor for Foundation.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_\$_AWEFriendsActivityWidgetConfigurationIntent |
| 2840 | 0x00b8e0b8 | 0x00b8e0b8 | GLOBAL | FUNC 0 | | _OBJC_METACLASS_\$_AWEFriendsActivityWidgetConfigurationIntentResponse |
| 2841 | 0x00b8e0e0 | 0x00b8e0e0 | GLOBAL | FUNC 0 | | _OBJC_METACLASS_\$_AWEFriendsActivityWidgetLandingPageResolutionResult |
| 2842 | 0x00b8e130 | 0x00b8e130 | GLOBAL | FUNC 0 | | _OBJC_METACLASS_\$_AWEFriendsWidgetsColorSchemeResolutionResult |
| 2843 | 0x00b8e068 | 0x00b8e068 | GLOBAL | FUNC 0 | | _OBJC_CLASS_\$_AWEFriendsActivityWidgetGetConfigurationIntent |
| 2844 | 0x00b8e090 | 0x00b8e090 | GLOBAL | FUNC 0 | | _OBJC_CLASS_\$_AWEFriendsActivityWidgetGetConfigurationIntentResponse |
| 2845 | 0x00b8e108 | 0x00b8e108 | GLOBAL | FUNC 0 | | _OBJC_CLASS_\$_AWEFriendsActivityWidgetGetLandingPageResolutionResult |
| 2846 | 0x00b8e158 | 0x00b8e158 | GLOBAL | FUNC 0 | | _OBJC_CLASS_\$_AWEFriendsWidgetsColorSchemeResolutionResult |
| 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

```

```

AwemeCore_rabin2_s.txt -- exportString
v18.9.0 > AwemeCore > AwemeCore_rabin2_s.txt
1 [Symbols]
2
3 nth paddr vaddr bind type size lib name
4
5 0 0x05614542 0x05614542 LOCAL FUNC 0 raddr://5614542
6 1 0x0cad6a38 0x11476a38 LOCAL FUNC 0 Foundation.NSNotFound.getter : Swift.Int
7 2 0x0cad6a44 0x11476a44 LOCAL FUNC 0 static Foundation.CharacterSet.whitespacesAndNewlines.gette
8 3 0x0cad6a50 0x11476a50 LOCAL FUNC 0 type metadata accessor for Foundation.CharacterSet
9 4 0x0cad6a5c 0x11476a5c LOCAL FUNC 0 static Foundation.Notification._unconditionallyBridgeFromO
10 5 0x0cad6a68 0x11476a68 LOCAL FUNC 0 Foundation.Notification.object.getter : Swift.Optional<Any>
11 6 0x0cad6a74 0x11476a74 LOCAL FUNC 0 Foundation.Notification.userInfo.getter : Swift.Optional<S
12 7 0x0cad6a88 0x11476a88 LOCAL FUNC 0 type metadata accessor for Foundation.Notification
13 8 0x0cad6a8c 0x11476a8c LOCAL FUNC 0 Foundation._convertErrorToNSError(Swift.Error) -> _C.NSERR
14 9 0x0cad6a98 0x11476a98 LOCAL FUNC 0 Foundation._convertNSErrorToNSError(Swift.Optional<_C.NSERRc
15 10 0x0cad6a4 0x11476a4 LOCAL FUNC 0 type metadata accessor for Foundation.NSFastEnumerationIter
16 11 0x0cad6ab 0x11476ab LOCAL FUNC 0 Foundation.URL.absoluteString.getter : Swift.String
17 12 0x0cad6ac 0x11476ac LOCAL FUNC 0 Foundation.URL_bridgeToObjective() -> _C.NSURL
18 13 0x0cad6a8 0x11476a8 LOCAL FUNC 0 static Foundation.URL._unconditionallyBridgeFromObjectiveC(
19 14 0x0cad6ad 0x11476ad LOCAL FUNC 0 Foundation.URL.scheme.getter : Swift.Optional<Swift.String>
20 15 0x0cad6ae 0x11476ae LOCAL FUNC 0 Foundation.URL.init(string: _shared Swift.String) -> Swift
21 16 0x0cad6ac 0x11476ac LOCAL FUNC 0 type metadata accessor for Foundation.URL
22 17 0x0cad6af 0x11476af LOCAL FUNC 0 Foundation.Data_copyContents(initializing: Swift.UnsafeMut
23 18 0x0cad6b0 0x11476b0 LOCAL FUNC 0 Foundation.Data_bridgeToObjectiveC() -> _C.NSData
24 19 0x0cad6b10 0x11476b10 LOCAL FUNC 0 static Foundation.Data._unconditionallyBridgeFromObjectiveC(
25 20 0x0cad6b1c 0x11476b1c LOCAL FUNC 0 type metadata accessor for Foundation.Data.Iterator
26 21 0x0cad6b28 0x11476b28 LOCAL FUNC 0 static Foundation.Date.distantPast.getter : Foundation.Date
27 22 0x0cad6b34 0x11476b34 LOCAL FUNC 0 Foundation.Date.timeIntervalSinceSince(Foundation.Date) -> Swift
28 23 0x0cad6b40 0x11476b40 LOCAL FUNC 0 Foundation.Date_bridgeToObjectiveC() -> _C.NSDate
29 24 0x0cad6b4c 0x11476b4c LOCAL FUNC 0 static Foundation.Date.> infix(Foundation.Date, Foundation.
30 25 0x0cad6b58 0x11476b58 LOCAL FUNC 0 Foundation.Date.init(timeIntervalSinceNow: Swift.Double) ->
31 26 0x0cad6b64 0x11476b64 LOCAL FUNC 0 Foundation.Date.init() -> Foundation.Date
32 27 0x0cad6b70 0x11476b70 LOCAL FUNC 0 type metadata accessor for Foundation.Date
33 28 0x0cad6b7c 0x11476b7c LOCAL FUNC 0 Foundation.UUID.randomUUID.getter : Swift.String
34 29 0x0cad6b88 0x11476b88 LOCAL FUNC 0 type metadata accessor for Foundation.UUID
35 30 0x0cad6b94 0x11476b94 LOCAL FUNC 0 Foundation.IndexPath_bridgeToObjectiveC() -> _C.NSIndexPa
36 31 0x0cad6ba0 0x11476ba0 LOCAL FUNC 0 static Foundation.IndexPath._unconditionallyBridgeFromObject
37 32 0x0cad6bac 0x11476bac LOCAL FUNC 0 (extension in UIKit):Foundation.IndexPath.init(row: Swift.I
38 33 0x0cad6bb8 0x11476bb8 LOCAL FUNC 0 (extension in UIKit):Foundation.IndexPath.row.getter : Swift
39 34 0x0cad6bc4 0x11476bc4 LOCAL FUNC 0 (extension in UIKit):Foundation.IndexPath.initItem: Swift
40 35 0x0cad6bd0 0x11476bd0 LOCAL FUNC 0 (extension in UIKit):Foundation.IndexPath.item.getter : Swift
41 36 0x0cad6bdc 0x11476bdc LOCAL FUNC 0 (extension in UIKit):Foundation.IndexPath.section.getter :
42 37 0x0cad6be8 0x11476be8 LOCAL FUNC 0 type metadata accessor for Foundation.IndexPath
43 38 0x0cad6hf4 0x11476hf4 LOCAL FUNC 0 static ObjectiveC.Selector._infix(Selector, Selector, Obj

```

-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.CharacterSet 0 0x11476a44"
"f sym.type_metadata_accessor_for_Foundation.CharacterSet 0 0x11476a50"
"f sym.static_Foundation.Notification._unconditionallyBridgeFromObjectiveC_Swift.Optional__C.NSNotification_____Foundation.Notification 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"
```

-1 : 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/VoicEngineRTC.framework/VoicEngineRTC
@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/sqlite3.dylib
/usr/lib/xml2.2.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 | AWComments |
| SwiftImpl | | | | | | | |
| 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  AWECommentsS
wiftImpl
22     0x00014530 0x00014530 8   9   1.__TEXT.__const      ascii  BaseCell
23     0x00014560 0x00014560 4   20  1.__TEXT.__const      utf32le A\nKí 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  AWECommentsS
wiftImpl
27     0x00014cc0 0x00014cc0 5   24  1.__TEXT.__const      utf32le 2\féh& 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  AWECommentsS
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 | AWEVideoMer
geTransParam |
| 39596 | 0x00f172ac | 0x00f172ac | 35 | 36 | 89 | __DATA.__objc_classname | ascii | AWEVideoNew
PublishCircleTagItemCell |
| 39597 | 0x00f172d0 | 0x00f172d0 | 38 | 39 | 89 | __DATA.__objc_classname | ascii | AWEVideoNew
PublishTagRecommendItemCell |
| 39598 | 0x00f172f7 | 0x00f172f7 | 43 | 44 | 89 | __DATA.__objc_classname | ascii | AWEVideoNew
PublishTagRecommendTableViewCell |
| 39599 | 0x00f17323 | 0x00f17323 | 12 | 13 | 89 | __DATA.__objc_classname | ascii | LVAudioFram
e |
| 39600 | 0x00f17330 | 0x00f17330 | 11 | 12 | 89 | __DATA.__objc_classname | ascii | Performance |
| 39601 | 0x00f1733c | 0x00f1733c | 12 | 13 | 89 | __DATA.__objc_classname | ascii | VoiceChange
r |
| 39602 | 0x00f17349 | 0x00f17349 | 32 | 33 | 89 | __DATA.__objc_classname | ascii | AWEVideoNew
PublishViewController |
| <hr/> | | | | | | | | |
| 119537 | 0xd7521ea | 0x120f21ea | 4 | 5 | 111 | __LTC_DATA._C_cstring | ascii | \t\bC |
| 119538 | 0xd752209 | 0x120f2209 | 7 | 9 | 111 | __LTC_DATA._C_cstring | utf8 | \ITjpS4 blo
cks Arabic, Basic Latin |
| 119539 | 0xd752246 | 0x120f2246 | 7 | 9 | 111 | __LTC_DATA._C_cstring | utf8 | n~0{P\fc bl
ocks Latin Extended-B, Basic Latin |
| 119540 | 0xd752252 | 0x120f2252 | 5 | 7 | 111 | __LTC_DATA._C_cstring | utf8 | ÈFyr' blocks
Cyrillic, Basic Latin |
| 119541 | 0xd75226f | 0x120f226f | 5 | 6 | 111 | __LTC_DATA._C_cstring | ascii | RS\rcJ |
| 119542 | 0xd752292 | 0x120f2292 | 4 | 5 | 111 | __LTC_DATA._C_cstring | ascii | o3PR |
| 119543 | 0xd7522da | 0x120f22da | 4 | 4 | 111 | __LTC_DATA._C_cstring | ascii | bvx\$ |

◀ ▶

-zr

→ AwemeCore rabin2 -zr ../../../../../已脱壳/v18.9.0/Payload/Aweme.app/Frameworks/AwemeCor
e.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 | 0x00000b9b0 | 0x84c0 | 0x00000b9b0 | 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_typerref |
| 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 | 0x0001dc4d | 0x0 | 0x0001dc4d | 0x0 | r-x | 6._TEXT.__cstring |
| 7 | 0x0001dc4d | 0x0 | 0x0001dc4d | 0x0 | r-x | 7._TEXT.__objc_methname |
| 8 | 0x0001dc4d | 0x0 | 0x0001dc4d | 0x0 | r-x | 8._TEXT.__objc_classname |
| 9 | 0x0001dc4d | 0x0 | 0x0001dc4d | 0x0 | r-x | 9._TEXT.__objc_methtype |
| 10 | 0x0001dc4d | 0x68 | 0x0001dc4d | 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_nlclstlist |
| 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.IESEliveBridge |
| 58 | 0x00d61710 | 0xa28 0x00d61710 | 0xa28 -rw- 58. __DATA.__bd_timsdk |
| 59 | 0x00d62138 | 0xf0 0x00d62138 | 0xf0 -rw- 59. __DATA.IESEliveTemplate |
| 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 | 0x13afffc 0x00e1100a | 0x13afffc -rw- 89 .__DATA.__objc_classname |
| 90 | 0x00f4c008 | 0x34840 0x00f4c008 | 0x34840 -rw- 90 .__DATA.__thread_bss |
| 91 | 0x0000000000 | 0x0 0x00f80860 | 0x2d6fe0 -rw- 91 .__DATA._D_tconst |
| 92 | 0x0000000000 | 0x0 0x01257840 | 0x3c3558 -rw- 92 .__DATA._D_dconst |
| 93 | 0x0000000000 | 0x0 0x0161c000 | 0x1225fc -rw- 93 .__DATA._D_ddata |
| 94 | 0x0000000000 | 0x0 0x0173e600 | 0x499b00 -rw- 94 .__DATA._D_cfstring |
| 95 | 0x0000000000 | 0x0 0x01bd8100 | 0x1c10870 -rw- 95 .__DATA._D_objc_const |
| 96 | 0x0000000000 | 0x0 0x037e8970 | 0xaeee4 -rw- 96 .__DATA._D_objc_ivar |
| 97 | 0x0000000000 | 0x0 0x03893858 | 0x2054c8 -rw- 97 .__DATA._D_objc_selrefs |
| 98 | 0x0000000000 | 0x0 0x03a98d20 | 0x4b5df0 -rw- 98 .__DATA._D_gcc_except_ta |
| 99 | 0x0000000000 | 0x0 0x03f4eb10 | 0x896683 -rw- 99 .__DATA._D_cstring |
| 100 | 0x0000000000 | 0x0 0x047e5194 | 0x7795a -rw- 100 .__DATA._D_ustring |
| 101 | 0x0000000000 | 0x0 0x0485caee | 0xae06ba -rw- 101 .__DATA._D_objc_methname |
| 102 | 0x0000000000 | 0x0 0x0533d1a8 | 0x1ca962 -rw- 102 .__DATA._D_objc_methtype |
| 103 | 0x0000000000 | 0x0 0x05507c00 | 0x17fc48 -rw- 103 .__DATA.__common |
| 104 | 0x0000000000 | 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/AwemeCore.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 0x0001dcfd4"
"f section.7.__TEXT.__objc_methname 1 0x0001dcfd4"
"f section.8.__TEXT.__objc_classname 1 0x0001dcfd4"
"f section.9.__TEXT.__objc_methtype 1 0x0001dcfd4"
"f section.10.__TEXT.__gcc_except_tab 1 0x0001dcfd4"
"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.IESELiveBridge 1 0x00d61590"
"f section.58.__DATA.__bd_timsdk 1 0x00d61710"
"f section.59.__DATA.IESELiveTemplate 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_iden
tification.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 | 0x00003b124 | NONE FUNC | CC_MD5 |

| | | | | |
|----|------------|------|----------------|---------------------------------|
| 1 | 0x0003b134 | NONE | FUNC | MGCopyAnswer |
| 2 | 0x0003b144 | NONE | FUNC | MSHookFunction |
| 3 | 0x0003b154 | NONE | FUNC | MSHookMessageEx |
| 4 | 0x0003b164 | NONE | FUNC | NSclassFromString |
| 5 | 0x00000000 | NONE | FUNC | NSFileSystemFreeSize |
| 6 | 0x0003b174 | NONE | FUNC | NSHomeDirectory |
| 7 | 0x00000000 | NONE | OBJC_CLASS | ASIIdentifierManager |
| 8 | 0x00000000 | NONE | OBJC_CLASS | NSBundle |
| 9 | 0x00000000 | NONE | OBJC_CLASS | NSData |
| 10 | 0x00000000 | NONE | OBJC_CLASS | NSDate |
| 11 | 0x00000000 | NONE | OBJC_CLASS | NSDateFormatter |
| 12 | 0x00000000 | NONE | OBJC_CLASS | NSDictionary |
| 13 | 0x00000000 | NONE | OBJC_CLASS | NSFileManager |
| 14 | 0x00000000 | NONE | OBJC_CLASS | NSJSONSerialization |
| 15 | 0x00000000 | NONE | OBJC_CLASS | NSMutableData |
| 16 | 0x00000000 | NONE | OBJC_CLASS | NSMutableDictionary |
| 17 | 0x00000000 | NONE | OBJC_CLASS | NSMutableString |
| 18 | 0x00000000 | NONE | OBJC_CLASS | NSMutableURLRequest |
| 19 | 0x00000000 | NONE | OBJC_CLASS | NSNumber |
| 20 | 0x00000000 | NONE | OBJC_CLASS | NSObject |
| 21 | 0x00000000 | NONE | OBJC_CLASS | NSString |
| 22 | 0x00000000 | NONE | OBJC_CLASS | NSTimeZone |
| 23 | 0x00000000 | NONE | OBJC_CLASS | NSURL |
| 24 | 0x00000000 | NONE | OBJC_CLASS | NSURLConnection |
| 25 | 0x00000000 | NONE | OBJC_CLASS | NSURLRequest |
| 26 | 0x00000000 | NONE | OBJC_CLASS | NSURLSession |
| 27 | 0x00000000 | NONE | OBJC_CLASS | NSURLSessionConfiguration |
| 28 | 0x00000000 | NONE | OBJC_CLASS | UIDevice |
| 29 | 0x00000000 | NONE | OBJC_METACLASS | NSObject |
| 30 | 0x0003b184 | NONE | FUNC | _Block_object_assign |
| 31 | 0x0003b194 | NONE | FUNC | _Block_object_dispose |
| 32 | 0x00000000 | NONE | FUNC | _NSConcreteGlobalBlock |
| 33 | 0x00000000 | NONE | FUNC | _NSConcreteStackBlock |
| 34 | 0x0003b1a4 | NONE | FUNC | _Unwind_SjLj_Register |
| 35 | 0x0003b1b4 | NONE | FUNC | _Unwind_SjLj_Resume |
| 36 | 0x0003b1c4 | NONE | FUNC | _Unwind_SjLj_Unregister |
| 37 | 0x00000000 | NONE | FUNC | _CFConstantStringClassReference |
| 38 | 0x0003b1d4 | NONE | FUNC | _assert_rtn |
| 39 | 0x00000000 | NONE | FUNC | _gxx_personality_sj0 |
| 40 | 0x00000000 | NONE | FUNC | _objc_personality_v0 |
| 41 | 0x0003b1e4 | NONE | FUNC | _stack_chk_fail |
| 42 | 0x00000000 | NONE | FUNC | _stack_chk_guard |
| 43 | 0x0003b1f4 | NONE | FUNC | _dyld_get_image_vmaddr_slide |
| 44 | 0x00000000 | NONE | FUNC | _objc_empty_cache |
| 45 | 0x0003b204 | NONE | FUNC | dispatch_async |
| 46 | 0x0003b214 | NONE | FUNC | dispatch_get_global_queue |
| 47 | 0x0003b224 | NONE | FUNC | dispatch_semaphore_create |
| 48 | 0x0003b234 | NONE | FUNC | dispatch_semaphore_signal |
| 49 | 0x0003b244 | NONE | FUNC | dispatch_semaphore_wait |
| 50 | 0x0003b254 | NONE | FUNC | dispatch_time |
| 51 | 0x0003b264 | NONE | FUNC | dclose |
| 52 | 0x0003b274 | NONE | FUNC | dlopen |
| 53 | 0x0003b284 | NONE | FUNC | dlsym |
| 54 | 0x0003b294 | NONE | FUNC | exit |
| 55 | 0x0003b2a4 | NONE | FUNC | free |
| 56 | 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 | strrstr |
| 73 | 0x0003b3c4 | NONE | FUNC | syscall |
| 74 | 0x0003b3d4 | NONE | FUNC | sysctl |
| 75 | 0x0003b3e4 | NONE | FUNC | uname |
| 76 | 0x00000000 | NONE | FUNC | dylld_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_\$_NbGzsksqtAxBgN |
| 1 | 0x0004084c | 0x0003c84c | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_NxNRxsBxexSx |
| 2 | 0x00040874 | 0x0003c874 | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_daAxbxbayGwxtxdcca |
| 3 | 0x000408c4 | 0x0003c8c4 | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_xrxeWZnuCXPEX |
| 4 | 0x000408ec | 0x0003c8ec | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_xxWxKxrETCxJpx |
| 5 | 0x00040888 | 0x0003c888 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_NbGzsksqtAxBgN |
| 6 | 0x00040838 | 0x0003c838 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_NxNRxsBxexSx |
| 7 | 0x00040860 | 0x0003c860 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_daAxbxbayGwxtxdcca |
| 8 | 0x000408b0 | 0x0003c8b0 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_xrxeWZnuCXPEX |
| 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_libraries.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_strings.txt
```

输出：

| | 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 | advertisingIdentifier | |
| 9 | 0x0003b6b2 | 0x0003b6b2 | 29 | 30 | 3. | __TEXT,__objc_methname | ascii | dictionaryWithObjectAndKeys: | |
| 10 | 0x0003b6d0 | 0x0003b6d0 | 14 | 15 | 3. | __TEXT,__objc_methname | ascii | URLWithString: | |
| 11 | 0x0003b6df | 0x0003b6df | 39 | 40 | 3. | __TEXT,__objc_methname | ascii | stringWithContentsOfURL:encoding:error: | |
| 12 | 0x0003b707 | 0x0003b707 | 10 | 11 | 3. | __TEXT,__objc_methname | ascii | hasPrefix: | |
| 13 | 0x0003b712 | 0x0003b712 | 24 | 25 | 3. | __TEXT,__objc_methname | ascii | deleteCharactersInRange: | |
| 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:options: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 PHcNExxxUJIxH
23 0x0003b7dd 0x0003b7dd 14 15 3.__TEXT.__objc_methname ascii graGqxxPtxaoBY
24 0x0003b7ec 0x0003b7ec 14 15 3.__TEXT.__objc_methname ascii xHvTCxxxxXVxm
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 resolveNetworkProbl
emForAppWithBundleId:
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 componentsSeparatedBy
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 0x0003bab9 0x0003bab9 14 15 3.__TEXT.__objc_methname ascii setHTTPMethod:
57 0x0003bac4 0x0003bac4 28 29 3.__TEXT.__objc_methname ascii setValue:forHTTPHeader
Field:
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 dataWithContentsOfFile
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 xKxcixmmxdPxZ
76 0x0003bc56 0x0003bc56 15 16 3.__TEXT.__objc_methname ascii xKxcixmmxdPxZ:
77 0x0003bc66 0x0003bc66 15 16 3.__TEXT.__objc_methname ascii MxJgqzxvqFtQxV:
78 0x0003bc76 0x0003bc76 37 38 3.__TEXT.__objc_methname ascii dVxAx1NLgYxxYh: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 0x0003bcbe 0x0003bcbe 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 xMREwdxMxkhxxx:
88 0x0003bd54 0x0003bd54 19 20 3.__TEXT.__objc_methname ascii appendBytes:length:
89 0x0003bd68 0x0003bd68 15 16 3.__TEXT.__objc_methname ascii LUxxxxfWDhvpGxJ:
90 0x0003bd78 0x0003bd78 15 16 3.__TEXT.__objc_methname ascii fexkIvlCfxhxsy:
91 0x0003bd88 0x0003bd88 14 15 3.__TEXT.__objc_methname ascii MjOhDBJSUcxxu
92 0x0003bd97 0x0003bd97 14 15 3.__TEXT.__objc_methname ascii gxcyxmxIxNux
93 0x0003bda6 0x0003bda6 14 15 3.__TEXT.__objc_methname ascii Ox1pxkxxFLzEnr
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 xtxNTxxxssVGxk
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"40"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 NxNXRxsBxexSx
1 0x0003bec0 0x0003bec0 18 19 5.__TEXT.__objc_classname ascii daAxbxbayGwxtxdcca
2 0x0003bed3 0x0003bed3 14 15 5.__TEXT.__objc_classname ascii NbGzxsksqtAxBgN
3 0x0003bee2 0x0003bee2 14 15 5.__TEXT.__objc_classname ascii xrxleWZnuCXPEEx
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^i16@20
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_\$_NbGzxsksqtAxBgN |
| 1 | 0x0004084c | 0x0003c84c | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_NxNXRxsBxexSx |
| 2 | 0x00040874 | 0x0003c874 | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_daAxbxbayGwxtxdcca |
| 3 | 0x000408c4 | 0x0003c8c4 | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_xrxleWZnuCXPEEx |
| 4 | 0x000408ec | 0x0003c8ec | GLOBAL | FUNC | 0 | | _OBJC_CLASS_\$_xxWxKxrETCxJpx |
| 5 | 0x00040888 | 0x0003c888 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_NbGzxsksqtAxBgN |
| 6 | 0x00040838 | 0x0003c838 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_NxNXRxsBxexSx |
| 7 | 0x00040860 | 0x0003c860 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_daAxbxbayGwxtxdcca |
| 8 | 0x000408b0 | 0x0003c8b0 | GLOBAL | FUNC | 0 | | _OBJC_METACLASS_\$_xrxleWZnuCXPEEx |
| 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 0x0003bia4 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_vaddr_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_sections.txt
```

输出：

[Sections]

| nth | paddr | size | vaddr | vsiz | 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 | 0xbc | -rw- | 21.__DATA.__common |
| 22 | 0x00040000 | 0x1 | 0x00040000 | 0x1 | -rw- | 22.__LLVM.__bundle |

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-05 16:29:02

rabin2的help语法

```

→ ~ rabin2 --help
rabin2: illegal option -- -
Usage: rabin2 [-AcdeEghHijlLMqrRsUVvXzz] [-@ 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 -SMZIHVResizeld -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: otool
 - 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

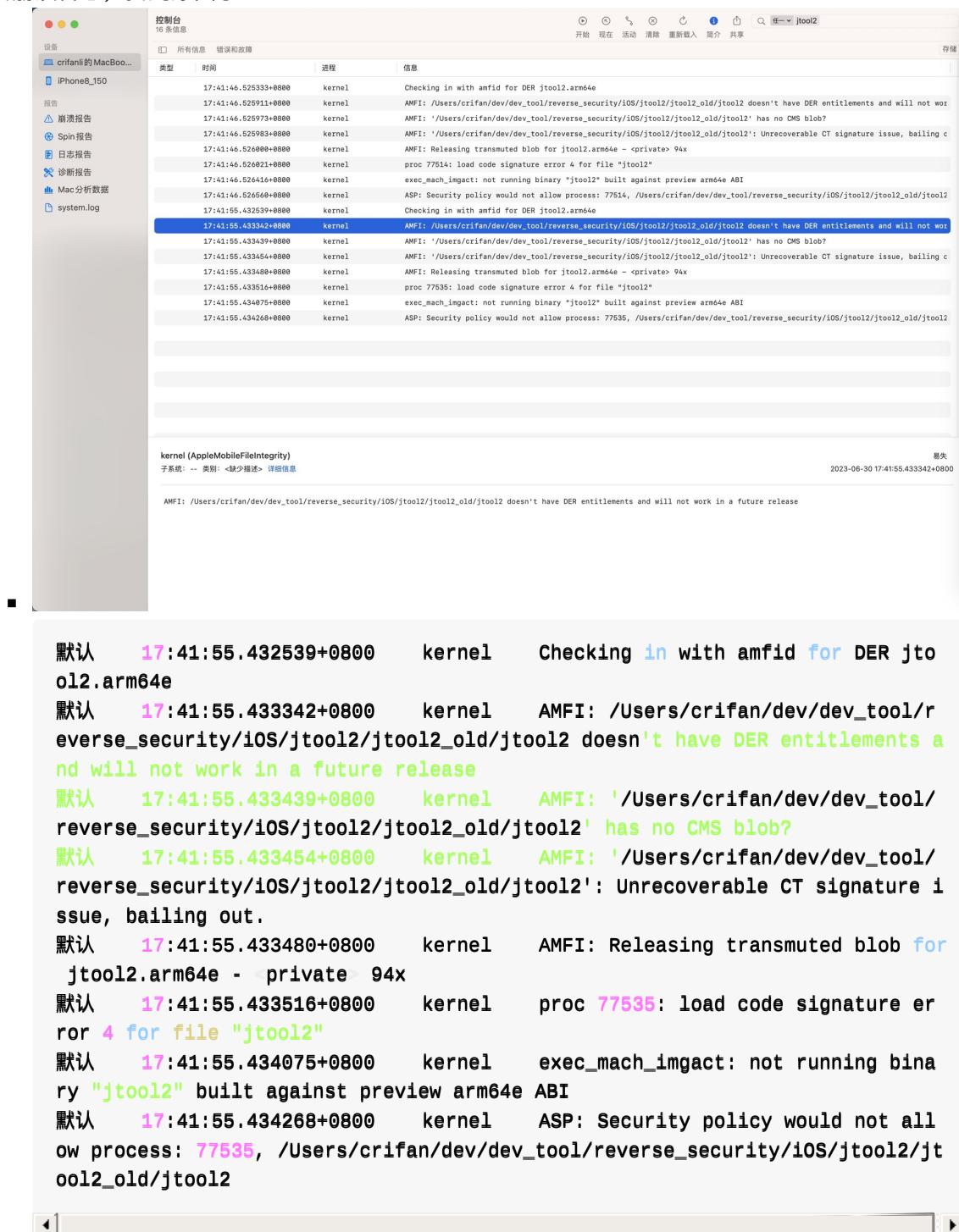
- 问题: Mac M2 Max + macOS Ventura 13.2.1 中, 用brew安装的原始版本=[官网版本的jtool2](#), 运行

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

◦ 找崩溃日志，找到原因了



• 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 \(newosxbook.com\)](https://newosxbook.com/jtool2-taking-the-o-out-of-otool-squared.html)

常见命令的常见用法举例

官网[JTool2 - Taking the O out of otool - squared \(newosxbook.com\)](https://newosxbook.com/jtool2-taking-the-o-out-of-otool-squared.html)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](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 23:20:43

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-05 16:48:12

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/AwemeCore
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: 0x0000000000-0x304000    __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: 0x00001da48-0x00001dc4  __TEXT.__swift5_types
  Mem: 0x00001dc4-0x00001dc4  __TEXT.__cstring  (C-String Literals)
  Mem: 0x00001dc4-0x00001dc4  __TEXT.__objc_methname  (C-String Literals)
  Mem: 0x00001dc4-0x00001dc4  __TEXT.__objc_classname  (C-String Literals)
  Mem: 0x00001dc4-0x00001dc4  __TEXT.__objc_methtype  (C-String Literals)
  Mem: 0x00001dc4-0x00001dd3c  __TEXT.__gcc_except_tab
  Mem: 0x00001dd40-0x00002136c  __TEXT.__swift5_refistr
  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.__cstring
  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_nlcattlist (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.XBMEexternal |
| 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.IESELiveBridge |
| Mem: 0x000d61710-0x000d62138 | __DATA.__bd_timsdk |
| Mem: 0x000d62138-0x000d62228 | __DATA.IESELiveTemplate |
| 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.XBMIInternal
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: 0x005924000-0x011476a38      Mem: 0x005924000-0x11480000      __BD_TEXT
Mem: 0x011476a38-0x01147ef40      __BD_TEXT.__text   (Normal)
                                         __BD_TEXT.__stubs  (Symbol Stubs)

LC 03: LC_SEGMENT_64
Mem: 0x011480000-0x011480208      Mem: 0x011480000-0x12660000      __LTC_DATA
Mem: 0x011480208-0x011480218      __LTC_DATA.__meta
Mem: 0x011480218-0x011b54d57      __LTC_DATA.__deco
Mem: 0x011b54d57-0x011b6eadf      __LTC_DATA._C_objc_const
Mem: 0x011b6eadf-0x0120f22de      __LTC_DATA._C_objc_ivar
Mem: 0x0120f22de-0x01232e92d      __LTC_DATA._C_cstring
Mem: 0x01232e92d-0x01257b342      __LTC_DATA._C_tconst
Mem: 0x01257b342-0x01265c5da      __LTC_DATA._C_gcc_except_ta
                                         __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 0xdffa63c0

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/AdServices
LC 17: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/AppTrackingTransparency.framework/AppTrackingTransparency
LC 18: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/AuthenticationServices.framework/AuthenticationServices
LC 19: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/CoreHaptics.framework/CoreHaptics
LC 20: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/CoreTelephony.framework/CoreTelephony
LC 21: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/MetalKit.framework/MetalKit
LC 22: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/MetalPerformanceShaders.framework/MetalPerformanceShaders
LC 23: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/MetricKit.framework/MetricKit
LC 24: LC_LOAD_WEAK_DYLIB      /System/Library/Frameworks/StoreKit.framework/StoreKit
LC 25: LC_LOAD_DYLIB           @rpath/VoicEngineRTC.framework/VoicEngineRTC
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/libsqllite3.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/AVFoundation
LC 39: LC_LOAD_DYLIB           /System/Library/Frameworks/AVKit.framework/AVKit
LC 40: LC_LOAD_DYLIB           /System/Library/Frameworks/Accelerate.framework/Accelerate
LC 41: LC_LOAD_DYLIB           /System/Library/Frameworks/AdSupport.framework/AdSupport
LC 42: LC_LOAD_DYLIB           /System/Library/Frameworks/AddressBook.framework/AddressBook
LC 43: LC_LOAD_DYLIB           /System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary
LC 44: LC_LOAD_DYLIB           /System/Library/Frameworks/AudioToolbox.framework/AudioToolbox
LC 45: LC_LOAD_DYLIB           /System/Library/Frameworks/CFNetwork.framework/CFNetwork
LC 46: LC_LOAD_DYLIB           /System/Library/Frameworks/Contacts.framework/Contacts
LC 47: LC_LOAD_DYLIB           /System/Library/Frameworks/ContactsUI.framework/ContactsUI
LC 48: LC_LOAD_DYLIB           /System/Library/Frameworks/CoreAudio.framework/CoreAudio
LC 49: LC_LOAD_DYLIB           /System/Library/Frameworks/CoreAudioKit.framework/CoreAudioKit
LC 50: LC_LOAD_DYLIB           /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation

```

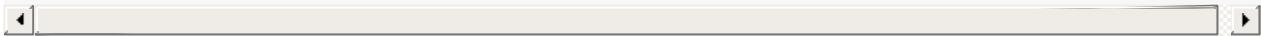
| | |
|---------------------------|--|
| LC 51: LC_LOAD_DYLIB | /System/Library/Frameworks/CoreGraphics.framework/Core |
| Graphics | |
| LC 52: LC_LOAD_DYLIB | /System/Library/Frameworks/CoreImage.framework/CoreIma |
| ge | |
| LC 53: LC_LOAD_DYLIB | /System/Library/Frameworks/CoreLocation.framework/Core |
| 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.framework |
| 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.framework |
| rk/LocalAuthentication | |
| LC 70: LC_LOAD_DYLIB | /System/Library/Frameworks/MapKit.framework/MapKit |
| LC 71: LC_LOAD_DYLIB | /System/Library/Frameworks/MediaAccessibility.framework |
| 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/OpenGL ES |
| 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.framework |

```

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/libswifttos.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 version 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/AppTrackingTransparency (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 version 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/MetalPerformanceShaders (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/VoIcEngineRTC.framework/VoIcEngineRTC (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, current version 1.0.0)
/System/Library/Frameworks/AVFoundation.framework/AVFoundation (compatibility version 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/OpenGL.framework/OpenGL (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/UIKit.framework/UIKit (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：

```

AwemeCore_jtool2_S.txt -- exportString
v18.9.0 > AwemeCore > AwemeCore_nm.txt
4989 U _xmlFreeDoc
4990 U _xmlFreeNode
4991 U _xmlFreeNs
4992 U _xmlFreeNsList
4993 U _xmlFreeParserCtxt
4994 U _xmlGetProp
4995 U _xmlHasNsProp
4996 U _xmlHasProp
4997 U _xmlInitParser
4998 U _xmlNewDoc
4999 U _xmlNewNode
5000 U _xmlNewNs
5001 U _xmlNewNsProp
5002 U _xmlNewProp
5003 U _xmlNewText
5004 U _xmlNextElementSibling
5005 U _xmlNodeDump
5006 U _xmlNodeGetContent
5007 U _xmlNodeListGetString
5008 U _xmlNodeSetContent
5009 U _xmlNodeSetName
5010 U _xmlParseChunk
5011 U _xmlReadMemory
5012 U _xmlSearchNs
5013 U _xmlSearchNsByHref
5014 U _xmlSetNs
5015 U _xmlSetTreeDoc
5016 U _xmlStrEqual
5017 U _xmlStrcmp
5018 U _xmlStrdup
5019 U _xmlStrlen
5020 U _xmlStrsub
5021 U _xmlUnlinkNode
5022 U _xmlXPathEval
5023 U _xmlXPathFreeContext
5024 U _xmlXPathFindObject
5025 U _xmlXPathNewContext
5026 U _xmlXPathRegisterNs
5027 U _zlibCompileFlags
5028 U _zlibVersion
5029 U dyld_stub_binder
5030

AwemeCore_nm.txt
4989 U _xmlFreeDoc
4990 U _xmlFreeNode
4991 U _xmlFreeNs
4992 U _xmlFreeNsList
4993 U _xmlFreeParserCtxt
4994 U _xmlGetProp
4995 U _xmlHasNsProp
4996 U _xmlHasProp
4997 U _xmlInitParser
4998 U _xmlNewDoc
4999 U _xmlNewNode
5000 U _xmlNewNs
5001 U _xmlNewNsProp
5002 U _xmlNewProp
5003 U _xmlNewText
5004 U _xmlNextElementSibling
5005 U _xmlNodeDump
5006 U _xmlNodeGetContent
5007 U _xmlNodeListGetString
5008 U _xmlNodeSetContent
5009 U _xmlNodeSetName
5010 U _xmlParseChunk
5011 U _xmlReadMemory
5012 U _xmlSearchNs
5013 U _xmlSearchNsByHref
5014 U _xmlSetNs
5015 U _xmlSetTreeDoc
5016 U _xmlStrEqual
5017 U _xmlStrcmp
5018 U _xmlStrdup
5019 U _xmlStrlen
5020 U _xmlStrsub
5021 U _xmlUnlinkNode
5022 U _xmlXPathEval
5023 U _xmlXPathFreeContext
5024 U _xmlXPathFindObject
5025 U _xmlXPathNewContext
5026 U _xmlXPathRegisterNs
5027 U _zlibCompileFlags
5028 U _zlibVersion
5029 U dyld_stub_binder
5030

```

--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 _$s10Foundation9IndexPathVSEAMc
0x40 _$s10Foundation9IndexPathVSQAMc

```

```

0x48 _$s10Foundation9IndexPathVSeAAMc |
0x50 _$s10ObjectiveC8ObjCBoolVMn |
0x58 _$s12CoreGraphics14CGPathFillRule07windingyA2CmFWC |
0x60 _$s12CoreGraphics7CGFloatVMn |
0x68 _$s12CoreGraphics7CGFloatVN |
0xd8 _$s15GroupActivities0A13StateObserverCMn |
0xe0 _$s15GroupActivities0A16ActivityMetadataVMA |
0xe8 _$s15GroupActivities0A16ActivityMetadataVMn |
0xf0 _$s15GroupActivities0A16ActivityMetadataVSEAAAC |
0xf8 _$s15GroupActivities0A16ActivityMetadataVSeAAMc |
0x100 _$s15GroupActivities0A16SessionMessengerC14MessageContextVMn |
0x108 _$s15GroupActivities0A16SessionMessengerC4send_2toyx_AA12Participants0tYaKSeRzSER
z1FTu |
0x110 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVMA |
0x118 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVMn |
0x120 _$s15GroupActivities0A16SessionMessengerC8MessagesV8IteratorVy_x_GSciIAAMc |
0x128 _$s15GroupActivities0A16SessionMessengerC8MessagesVMA |
0x130 _$s15GroupActivities0A16SessionMessengerC8MessagesVMn |
0x138 _$s15GroupActivities0A16SessionMessengerC8MessagesVy_xGSciIAAMc |
0x140 _$s15GroupActivities0A16SessionMessengerCMn |
0x148 _$s15GroupActivities0A24ActivityActivationResult018activationDisabledyA2CmFWC |
0x150 _$s15GroupActivities0A24ActivityActivationResult019activationPreferedyA2CmFWC |
0x158 _$s15GroupActivities0A24ActivityActivationResult09cancelleydA2CmFWC |
0x160 _$s15GroupActivities0A7SessionC3endyyF |
0x168 _$s15GroupActivities0A7SessionC5State011invalidatedyAEyx_Gs5Error_p_tcAGmAA0A8Act
ivityRzlFWC |
0x170 _$s15GroupActivities0A7SessionC5leaveyyF |
0x178 _$s15GroupActivities0A7SessionC8SessionsV8IteratorVyx__GSciIAAMc |
0x180 _$s15GroupActivities0A7SessionC8SessionsVyx_GSciIAAMc |
0x188 _$s15GroupActivities0A7SessionCMa |
0x190 _$s15GroupActivities0A7SessionCMn |
0x1a0 _$s15GroupActivities0A8ActivityPAAE20prepareForActivationAA0acF6Result0yYaFTu |
0x1a8 _$s15GroupActivities0A8ActivityPAAE8activateSbyYaKFTu |
0x1b0 _$s15GroupActivities11ParticipantVMA |
0x1b8 _$s15GroupActivities11ParticipantVMn |
0x1c0 _$s15GroupActivities11ParticipantVSHAAMc |
0x1c8 _$s15GroupActivities12Participants03allyA2CmFWC |
0x348 _$s7Combine10Publishers016RemoveDuplicatesVMn |
0x350 _$s7Combine10Publishers016RemoveDuplicatesVy_xGAA9PublisherAAMc |
0x358 _$s7Combine10Publishers03MapVMn |
0x360 _$s7Combine10Publishers03MapVy_xq_GAA9PublisherAAMc |
0x368 _$s7Combine10Publishers04DropVMn |
0x370 _$s7Combine10Publishers04DropVy_xGAA9PublisherAAMc |
0x378 _$s7Combine10Publishers09ReceiveOnVMn |
0x380 _$s7Combine10Publishers09ReceiveOnVy_xq_GAA9PublisherAAMc |
0x388 _$s7Combine14AnyCancellableCMn |
0x390 _$s7Combine9PublishedV9PublisherVMA |
0x398 _$s7Combine9PublishedV9PublisherVMn |
0x3a0 _$s7Combine9PublishedV9PublisherVy_x_GaadAMc |
0x3a8 _$s7Combine9PublishedVMA |
0x3b0 _$s7Combine9PublishedVMn |
0x3c8 _$s8Dispatch0A12TimeInterval012millisecondsyACSiCACmFWC |
0x3d0 _$s8Dispatch0A13WorkItemFlagsVMA |
0x3d8 _$s8Dispatch0A13WorkItemFlagsVMn |
0x3e0 _$s8Dispatch0A13WorkItemFlagsVs10SetAlgebraAAMc |
0x3e8 _$s8Dispatch0A3QoSV0B6SClass07defaultyA2EmFWC |

```

```

0x400 _$sBbWV
0x410 _$sSDMn
...
0xc1ae6f8 - [APMobileIdentifier IMSI]
0xc1ae704 - [APMobileIdentifier IMEI]
0xc1ae710 - [APMobileIdentifier TID]
0xc1ae71c - [APMobileIdentifier deviceFingerprint]
0xc1ae728 - [APMobileIdentifier UT DID]
0xc1ae734 - [APMobileIdentifier setUT DID:]
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 aewlynx_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 - [LynxUIScrollView sendScrollEvent:scrollTop:scrollLeft:scrollHeight:scrollWidth:deltaX:deltaY:]
0x11241f30 - [LynxUIScrollView contentSizeDidChange]
0x1124213c - [LynxUIScrollView clampScrollToPosition:]
0x1124224c - [LynxUIScrollView scrollTo:withResult:]
0x112424cc - [LynxUIScrollView autoScroll:withResult:]
0x112425ac - [LynxUIScrollView startAutoScrollWithRate:]
0x112426d4 - [LynxUIScrollView stopAutoScroll]
0x11242734 - [LynxUIScrollView dealloc]
0x112427b0 - [LynxUIScrollView frameDidChange]
0x1124286c - [LynxUIScrollView scrollLeftLimit]
0x11242900 - [LynxUIScrollView scrollRightLimit]
0x112429fc - [LynxUIScrollView scrollUpLimit]
0x11242a90 - [LynxUIScrollView scrollDownLimit]
0x11242b8c - [LynxUIScrollView canScroll:]
0x11242cb8 - [LynxUIScrollView scroll:direction:]
0x11242e04 - [LynxUIScrollView scrollByX:]
0x11242e14 - [LynxUIScrollView scrollByY:]
0x11242e24 - [LynxUIScrollView flick:direction:]
0x11243054 - [LynxUIScrollView flickX:]
0x11243064 - [LynxUIScrollView flickY:]
0x11243074 - [LynxUIScrollView enableSticky]
0x11243084 - [LynxUIScrollView setEnableSticky:]
0x11243094 - [LynxUIScrollView enableScrollY]
0x112430a4 - [LynxUIScrollView setEnableScrollY:]
0x112430b4 - [LynxUIScrollView .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 updateFontSize:]
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 reloadDataWithTemplateData:]
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:needLayout:]
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]

```

```
0x11247cf8 - [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`

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 11:40:54

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.t
xt
```

输出：

```
LC 00: LC_SEGMENT_64           Mem: 0x0000000000-0x40000    __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: 0x00003fee4-0x00003ffff4 __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.dylib
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 (0x4cf40-0x4fc0)
LC 22: LC_DATA_IN_CODE             Offset: 315328, Size: 0 (0x4fc0-0x4fc0)
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, current version 61000.0.0)
/System/Library/Frameworks/Foundation.framework/Foundation (compatibility version 300.0.0, 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 version 150.0.0, current version 1677.104.0)
```

-S

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

输出：

```
00000000000040d28 D _OBJC_CLASS_$_NbGzxsksqtAsgN
00000000000040c88 D _OBJC_CLASS_$_NxNXRxsbBxexSx
00000000000040cd8 D _OBJC_CLASS_$_daAxbxbayGwtxdcca
00000000000040d78 D _OBJC_CLASS_$_xrxleWZnuCXPEx
00000000000040dc8 D _OBJC_CLASS_$_xxWxKxrETCxJpx
00000000000040d00 D _OBJC_METACLASS_$_NbGzxsksqtAsgN
00000000000040c60 D _OBJC_METACLASS_$_NxNXRxsbBxexSx
00000000000040cb0 D _OBJC_METACLASS_$_daAxbxbayGwtxdcca
00000000000040d50 D _OBJC_METACLASS_$_xrxleWZnuCXPEx
00000000000040da0 D _OBJC_METACLASS_$_xxWxKxrETCxJpx
00000000000044fb4 S _g_slide
000000000000450f8 S _x
000000000000450fc S _x.146
...
00000000000044fdc S _y.382
    U _CC_MD5
    U _MGCopyAnswer
    U _MSHookFunction
    U _MSHookMessageEx
    U _NSClassFromString
    U _NSFileSystemFreeSize
    U _NSHomeDirectory
    U _OBJC_CLASS_$_ASIIdentifierManager
    U _OBJC_CLASS_$_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 __strrstr
```

```

U _syscall
U _sysctl
U _uname
U dyld_stub_binder

```

--analyze

```

→ DynamicLibraries jtool2 --analyze MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_analyze.txt
Analyzing file...
processLoadCommands: Not a Mach-O magic (0xbebacfa)
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 MaskProDylib/MaskProDylib_jtool2_analyze.txt

```

输出：

```

MaskProDylib_jtool2_analyze.coffee — Mask
mtool -l MaskPro.dylib > MaskProDylib/MaskProDylib_jtool2_analyze.txt
Library > MobileSubstrate > DynamicLibraries > MaskProDylib > MaskProDylib_jtool2_analyze.coffee
1 0x19[0x666] | architecture Aa ab * 无结果 ↑ ↓ ≡ ×
2 0x78e4-[NNXRxsBxexSx eKGEGSRxxxPxt] |
3 0x95fc-[NNXRxsBxexSx PhchNxxuIxxH] |
4 0x9848-[NNXRxsBxexSx graGpxxPxaoBY] |
5 0x9a94-[NxNRxsBxexSx xHvTCxxxxxVm] |
6 0xb780-[NNXRxsBxexSx xWlxspxxExaux] |
7 0x22b54-[dAxAxbayGwxtdcca setAppWirelessDataOption:forBundleIdentifier:completionHandler:] |
8 0x22ff4-[dAxAxbayGwxtdcca setAppCellularDataEnabled:forBundleIdentifier:completionHandler:] |
9 0x233a0-[dAxAxbayGwxtdcca setUsagePoliciesForBundle:cellular:wifi:] |
10 0x330b8-[xxNxKxrETCxJpx xouxFivloloYFx] |
11 0x3453c-[xxNxKxrETCxJpx Mj0hD8JSUlcxxxx] |
12 0x34814-[xxNxKxrETCxJpx gxcymxxxxIxNux] |
13 0x34ab8-[xxNxKxrETCxJpx xtNTtxxxvGxk] |
14 0x34d68-[xxNxKxrETCxJpx 0xlpkxxFLzEnr] |
15 0x34ff8-[xxNxKxrETCxJpx fd]cxxxxt]xWeL] |
16 0x40000,_NSfileSystemFreeSize |
17 0x40008,_NSConcreteStackBlock |
18 0x40018,__gx_per الشخصية_v0 |
19 0x40018,__objc_per الشخصية_v0 |
20 0x40020,__stack_chk_guard |
21 0x40028,dyld_stub_binder |
22 0x40030,_CC_MDS |
23 0x40038,_MGCopyAnswer |
24 0x40040,_MSHookFunction |
25 0x40048,_MSHookMessageEx |
26 0x40050,_NSClassFromString |
27 0x40058,_NSHomeDirectory |
28 0x40060,_Block_object_assign |
29 0x40068,_Block_object_Dispose |
30 0x40070,_Unwind_Resume |
31 0x40078,__assert_rtn |
32 0x40080,__stack_chk_fail |
33 0x40088,__dyld_get_image_vmaddr_slide |
34 0x40090,__bzero |
35 0x40098,__dispatch_async |
36 0x400a0,__dispatch_get_global_queue |
37 0x400a8,__dispatch_semaphore_create |
38 0x400b0,__dispatch_semaphore_signal |
39 0x400b8,__dispatch_semaphore_wait |
40 0x400c0,__dispatch_time |
41 0x400c8,__dlclose |
42 0x400d0,__dlopen |
43 0x400d8,__dlsym

```

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 23:21:11

akd

--pages

```
x crifan@licrifandeMacBook-Pro ~ /dev/dev_root/iosReverse/AppleStore/AuthKit_akd/AuthKi
t.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)
    0fec18-0xfec20 __DATA_CONST.__objc_catlist (8 bytes)
    0fec20-0xfed50 __DATA_CONST.__objc_protolist (304 bytes)
    0fed50-0xfed58 __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.__cstring (18432 bytes)
0xfe890-0xfc18 __DATA_CONST.__objc_classlist (904 bytes)
0xfc18-0xfc20 __DATA_CONST.__objc_catlist (8 bytes)
0xfc20-0xfd50 __DATA_CONST.__objc_protolist (304 bytes)
0xfd50-0xfed58 __DATA_CONST.__objc_imagineinfo (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)

```

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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：
2023-10-07 15:44:41

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 resigning 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, armv7, 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. Useful to watch these step-by-step |
| WITHSIGBLOB | Code signing: Also create an empty CMS blob (no longer a default due to CoreTrust) |

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-10-04 23:07:06

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：

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

当前版本：

```
x 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
thumbbeb   - 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 load commands

```
otool -l iOSBinaryFile
```

- L : print shared Libraries used

```
otool -L iOSBinaryFile
```

- o : print the Objective-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

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-05 16:05:36

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 0x00000000100007da0
    size 0x00000000000000108
    offset 32160
    align 2^2 (4)
    reloff 0
    nreloc 0
    flags 0x80000400
reserved1 0
reserved2 0

Section
    sectname __const
    segname __TEXT
    addr 0x00000000100007ea8
    size 0x000000000000000011
    offset 32424
    align 2^1 (2)
    reloff 0
    nreloc 0
    flags 0x00000000
reserved1 0
reserved2 0

Section
    sectname __cstring
    segname __TEXT
    addr 0x00000000100007eb9
    size 0x00000000000000009b
    offset 32441
    align 2^0 (1)
    reloff 0
    nreloc 0
    flags 0x00000002
reserved1 0
reserved2 0

Section
    sectname __unwind_info
    segname __TEXT
    addr 0x00000000100007f54
    size 0x0000000000000000ac
    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 0x00000000100008000
    vmsize 0x00000000000004000

```

```

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 0x000000000000000b8
        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 0x000000000000000b8
        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 0x00000000000208000
    fileoff 49152
    filesize 0
    maxprot 0x00000003
    initprot 0x00000003
    nsects 1
    flags 0x0
Section
    sectname __objc_selrefs
    segname __DATA_CONST
        addr 0x000000010000C000
        size 0x000000000002054d2
        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 0x00000000000000000000
    fileoff 49152
    filesize 0
    maxprot 0x00000001
    initprot 0x00000001
    nsects 1
    flags 0x0
Section
    sectname __message_refs
    segname __OBJC
        addr 0x0000000100214000
        size 0x00000000000000000000
        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 0x00000000000008000

```

```

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
    hindirectsyms 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
cmdsiz 16
version 10.0
sdk 15.0
Load command 12
    cmd LC_SOURCE_VERSION
cmdsiz 16
version 0.0
Load command 13
    cmd LC_MAIN
cmdsiz 24
entryoff 31896
stacksize 0
Load command 14
    cmd LC_ENCRYPTION_INFO_64
cmdsiz 24
cryptoff 28672
cryptsize 4096
cryptid 1
pad 0
Load command 15
    cmd LC_LOAD_DYLIB
cmdsiz 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
cmdsiz 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
cmdsiz 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
cmdsiz 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
cmdsiz 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
cmdsiz 32
    path /usr/lib/swift (offset 12)
Load command 21
    cmd LC_RPATH
cmdsiz 40
    path @executable_path/Frameworks (offset 12)
Load command 22
    cmd LC_FUNCTION_STARTS
cmdsiz 16
dataoff 49640
datasize 32
Load command 23
    cmd LC_DATA_IN_CODE
cmdsiz 16
dataoff 49672
datasize 0
Load command 24
    cmd LC_CODE_SIGNATURE
cmdsiz 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/1Phone7-137black/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)
```

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:
2023-10-07 11:14:31

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 11
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 0x00000000000017e90
size 0x00000000000002ef8
offset 97936
align 2^4 (16)
reloff 0
nreloc 0
flags 0x00000000
reserved1 0
reserved2 0
Section
sectname __swift5_fieldmd
segname __TEXT
addr 0x0000000000001ad88
size 0x00000000000002988
offset 109960
align 2^2 (4)
reloff 0
nreloc 0
flags 0x00000000
reserved1 0
reserved2 0
Section
sectname __swift5_proto
segname __TEXT
addr 0x0000000000001d710
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 0x0000000000001da48
size 0x000000000000028c
offset 121416
align 2^2 (4)
reloff 0
nreloc 0
flags 0x00000000
reserved1 0
reserved2 0
Section
sectname __cstring
segname __TEXT
addr 0x0000000000001dc4

```

```

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 0x00000000000000050
  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 0x00000000000000050
  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 0x000000000000006c0
  offset 14053544
  align 2^3 (8)

```

```

    reloff 0
    nreloc 0
    flags 0x00000013
reserved1 0
reserved2 0

. . .

Section
    sectname __D_ustring
    segname __DATA
        addr 0x000000000047e5194
        size 0x0000000000007795a
    offset 0
    align 2^1 (2)
    reloff 0
    nreloc 0
    flags 0x00000001
reserved1 0
reserved2 0

Section
    sectname __D_objc_methname
    segname __DATA
        addr 0x0000000000485caee
        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 0x0000000000533d1a8
        size 0x0000000000001ca962
    offset 0
    align 2^0 (1)
    reloff 0
    nreloc 0
    flags 0x00000001
reserved1 0
reserved2 0

Section
    sectname __common
    segname __DATA
        addr 0x00000000005507c00
        size 0x00000000000017fc48
    offset 0
    align 2^10 (1024)
    reloff 0
    nreloc 0
    flags 0x00000001
reserved1 0
reserved2 0

Section
    sectname __bss

```

```

segname __DATA
    addr 0x00000000005687900
    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 0x00000000005924000
    vmsize 0x00000000bb5c000
    fileoff 16269312
    filesize 196460544
    maxprot 0x00000005
    initprot 0x00000005
    nsects 2
    flags 0x0
Section
    sectname __text
    segname __BD_TEXT
    addr 0x00000000005924000
    size 0x00000000bb52a38
    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 0x00000000000008508
    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 0x000000000011e0000
    fileoff 212729856
    filesize 18743296
    maxprot 0x00000001
    initprot 0x00000001

```

```

nsects 8
flags 0x0

...
Section
sectname __C_gcc_except_ta
segname __LTC_DATA
addr 0x000000001232e92d
size 0x0000000000024ca15
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 0x000000000000e1298
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
cmdsiz 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
    locrel off 0
        nlocrel 0
Load command 9
    cmd LC_UUID
cmdsiz 24
    uuid F1FCF15A-6465-31F0-9300-5BA1B8F91017
Load command 10
    cmd LC_VERSION_MIN_IPHONEOS
cmdsiz 16
    version 10.0
    sdk 15.0
Load command 11
    cmd LC_SOURCE_VERSION
cmdsiz 16
    version 0.0
Load command 12
    cmd LC_ENCRYPTION_INFO_64
cmdsiz 24
    cryptoff 32768
    cryptsize 3112960
    cryptid 0
    pad 0
Load command 13
    cmd LC_LOAD_DYLIB
cmdsiz 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) :

```

otool_oV_AwemeCore.txt -- iPhone7P-1341
nm_AwemeCore.txt strings_AwemeCore_removeNoUse.txt otool_L_AwemeCore.txt otool_oV_AwemeCore.txt ...
Aweme.app > Frameworks > AwemeCore.framework > otool_oV_AwemeCore.txt
1 AwemeCore:
2 Contents of (_DATA,_objc_classlist) > _aweme
3 00000000003221c8 0x9acaf0
4 isa 0x9cac8
5 superclass 0x0 _OBJC_CLASS_$_NSObject
6 cache 0x0 __objc_empty_cache
7 vtable 0x0
8 data 0x37f798
9 flags 0x0
10 instanceStart 8
11 instanceSize 12
12 reserved 0x0
13 ivarLayout 0x0
14 name 0xe1100a BOLDDecompressor_AwemeCore
15 baseMethods 0x37f708
16 entsize 24
17 count 3
18 name 0xd86870 copyWithZone:
19 types 0xdf3478 @24@0:8^{_NSZone=}16
20 imp 0x5babaf0
21 name 0xd8d4267 foo
22 types 0xdf34a7 i16@0:8
23 imp 0x5bac0a0
24 name 0xd84298 setFoo:
25 types 0xdf34af v2@0:8@16
26 imp 0x5bac0a8
27 baseProtocols 0x37f6a8
28 count 1
29 list[0] 0x9bd758
30 isa 0x0
31 name 0xe11497 NSCopying
32 protocols 0x0
33 instanceMethods 0x38ffe8
34 entsize 24
35 count 1
36 name 0xd86870 copyWithZone:
37 types 0xdf3478 @24@0:8^{_NSZone=}16
38 imp 0x0
39 classMethods 0x0
40 optionalInstanceMethods 0x0
41 optionalClassMethods 0x0
42 instanceProperties 0x0
43 ivars 0x37f758

```

```

nm_AwemeCore.txt strings_AwemeCore_removeNoUse.txt otool_l_AwemeCore.txt otool_oV_AwemeCore.txt
Aweme.app > Frameworks > AwemeCore.framework > _aweme
1624049 isa 0x0
1624050 name 0x4bbac BDXVideoCorePlayerDelegate
1624051 protocols 0x0
1624052 instanceMethods 0x0
1624053 classMethods 0x0
1624054 optionalInstanceMethods 0x0
1624055 optionalClassMethods 0x0
1624056 instanceProperties 0x0
1624057 00000000037f638 0xd54bf0
1624058 isa 0x0
1624059 name 0x4bbc7 BDXVideoPlayProgressDelegate
1624060 protocols 0x0
1624061 instanceMethods 0x0
1624062 classMethods 0x0
1624063 optionalInstanceMethods 0x0
1624064 optionalClassMethods 0x0
1624065 instanceProperties 0x0
1624066 00000000037f640 0xd54d90
1624067 isa 0x0
1624068 name 0x4bc44 BDXVideoFullScreenPlayer
1624069 protocols 0x0
1624070 instanceMethods 0x0
1624071 classMethods 0x0
1624072 optionalInstanceMethods 0x0
1624073 optionalClassMethods 0x0
1624074 instanceProperties 0x0
1624075 00000000037f648 0xd55890
1624076 isa 0x0
1624077 name 0x4bf19 YYWebImageOperation
1624078 protocols 0x0
1624079 instanceMethods 0x0
1624080 classMethods 0x0
1624081 optionalInstanceMethods 0x0
1624082 optionalClassMethods 0x0
1624083 instanceProperties 0x0
1624084 Contents of (__DATA,__objc_selrefs) section
1624085 0xd84267 foo
1624086 Contents of (__DATA,__objc_imageinfo) section
1624087 version 0
1624088 flags 0x5010700 Swift 5 or later

```

```

AwemeCore:
Contents of (__DATA,__objc_classlist) section
0000000003221c8 0x9aca0
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 T1,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

```

```

000000000037f648 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_$_NSObject
cache 0x0 __objc_empty_cache
vtable 0x0
data 0x3921f8
flags 0x80
instanceStart 8
instanceSize 8
reserved 0x0
ivarLayout 0x0
name 0xe12aaaf AWECloudJailBreakUtility
baseMethods 0x0
baseProtocols 0x0
ivars 0x0
weakIvarLayout 0x0
baseProperties 0x0
Meta Class
isa 0x0 _OBJC_METACLASS_$_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 0xe12aaaf 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 `0xe12aaaf AwECloudJailBreakUtility`
  - >好像是：`AwECloudJailBreakUtility` 这个类的位置是 `0xe12aaaf`

-》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：`0xe12aaaf`

->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：

```

iPhone7P-1341
...
nm_AwemeCore.bundle ... nm_AwemeCore.txt strings_AwemeCore_removeNoUse.txt otool_l_AwemeCore.txt otool_oV_AwemeCore.txt ...
Aweme.app > Frameworks > AwemeCore.framework > _otool_oV_AwemeCore.txt
jail
28774 instanceStart 8
28775 instanceSize 8
28776 reserved 0x0
28777 ivarLayout 0x0
28778 name 0xe163f6 BDInstallNetworkUtility
28779 baseMethods 0x0
28780 baseProtocols 0x0
28781 ivars 0x0
28782 weakIvarLayout 0x0
28783 baseProperties 0x0
28784 Meta Class
28785 isa 0x0 _OBJC_METACLASS_$_NSObject
28786 superclass 0x0 _OBJC_METACLASS_$_NSObject
28787 cache 0x0 __objc_empty_cache
28788 vtable 0x0
28789 data 0x3a71e0
28790 flags 0x81 RO_META
28791 instanceStart 40
28792 instanceSize 40
28793 reserved 0x0
28794 ivarLayout 0x0
28795 name 0xe163f6 BDInstallNetworkUtility
28796 baseMethods 0x3a70e8
28797 entsize 24
28798 count 10
28799 name 0xd842dd load
28800 types 0xdf33c3 v16@0:8
28801 imp 0x5927654
28802 name 0xd8dbc6 onTheFlyParameter
28803 types 0xdf33de @16@0:8
28804 imp 0x5f800dc
28805 name 0xd8dc1d commonURLParameters
28806 types 0xdf33de @16@0:8
28807 imp 0x5f8e628
28808 name 0xd8dc31 buildQueryFromDictionary:
28809 types 0xdf3380 @24@0:8@16
28810 imp 0x5f8edf4
28811 name 0xd8dc83 isUpgradeUser
28812 types 0xdf3410 B16@0:8
28813 imp 0x5f8f07c
28814 name 0xd8c1d2 isJailBroken
28815 types 0xdf3410 B16@0:8

```

### 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=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

-1

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

输出：

```

450 cmd LC_LOAD_DYLIB
451 cmdsize 92
452 name /System/Library/Frameworks/CoreFoundation.framework/CoreFoundation (offset 24)
453 time stamp 2 Thu Jan 1 08:00:02 1970
454 current version 1677.104.0
455 compatibility version 150.0.0
456 Load command 21
457 cmd LC_FUNCTION_STARTS
458 cmdsize 16
459 dataoff 282540
460 datasize 124
461 Load command 22
462 cmd LC_DATA_IN_CODE
463 cmdsize 16
464 dataoff 282664
465 datasize 256
466 Load command 23
467 cmd LC_CODE_SIGNATURE
468 cmdsize 16
469 dataoff 288768
470 datasize 4112
471 MaskPro.dylib (architecture arm64):
472 Load command 0
473 cmd LC_SEGMENT_64
474 cmdsize 872
475 segname __TEXT
476 vmaddr 0x0000000000000000
477 vmsize 0x0000000000040000
478 fileoff 0
479 filesize 262144
480 maxprot 0x00000005
481 initprot 0x00000005
482 nsects 10
483 flags 0x0
484 Section
485 sectname __text
486 segname __TEXT
487 addr 0x00000000000078e4
488 size 0x0000000000036afc
489 offset 30948
490 align 2<2 (4)
491 reloff 0
492 nreloc 0

```

-OV

```
→ DynamicLibraries otool -ov MaskPro.dylib > MaskProDylib/MaskProDylib_otool_ov.txt
```

输出：

MaskProDylib\_otool\_oV.coffee — Mask

```

otool -l MaskProDylib > MaskProDylib/Ma Untitled-1 • MaskProDylib_otool_oV.coffee
Library > MobileSubstrate > DynamicLibraries > MaskProDylib > MaskProDylib_otool_oV.coffee
> architecture Aa ab * 第 2 项, 共 2 项 下 ≡
367 0x3b09 gcyxymxx1xNux
368 0x3bdab 0x1pxkxxfLzEnr
369 0x3bdab fDjCxxvTxjxWEl
370 0x3bde2 floatValue
371 0x3bded mainBundle
372 0x3bdf8 bundleIdentifier
373 0x3be0b resolveNetworkProblemForAppWithBundleId:
374 0x3be09 jailbrokenMask:
375 0x3be19 loadView
376 0x3be22 currentTitle
377 0x3b7ce PHNExxxUIJxxH
378 0x3b7dd graGqxxPttaoBY
379 0x3be21 dataWithBytes:length:
380 0x3b6d8 UXxxwDhpGx:
381 0x3bcd0 emqqxrXzxPuvx:::
382 0x3bd78 fexxk1vlCfxhsy:
383 0x3be45 UTF8String
384 0x3be50 requestWithURL:cachePolicy:timeoutInterval:
385 Contents of __DATA,__objc_imageinfo section
386 version 0
387 flags 0x40
388 MaskPro.dylib (architecture arm64):
389 Contents of __DATA,__objc_classlist section
390 0000000000402b0 0x40c88 _OBJC_CLASS_$_NxNRxsBbxexSx
391 isa 0x40c60 _OBJC_METACLASS_$_NxNRxsBbxexSx
392 superclass 0x0 _OBJC_CLASS_$_NSObject
393 cache 0x0 __objc_empty_cache
394 vtable 0x0
395 data 0x403a8
396 flags 0x80
397 instanceStart 8
398 instanceSize 8
399 reserved 0x0
400 ivarLayout 0x0
401 name 0x3fb3e NxNRxsBbxexSx
402 baseMethods 0x40328
403 entsize 24
404 count 5
405 name 0x3f44b eKGEGRxxxPx
406 types 0x3fb8d @16@0:8
407 imp 0x78e4
408 name 0x3f45a PhchExxxUITxxH
409 types 0x3fb8d @16@0:8

```

行 388, 列 29 (已选择13) 空格: 4 UTF-8 LF CoffeeScript ⚙ Prettier ⌂ ⌂

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新:

2023-10-07 23:21:52

## otool的help语法

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

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

## man手册

|                                                                                                                                                                                                                                                                                                                                                     |                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <b>PAGESTUFF(1)</b>                                                                                                                                                                                                                                                                                                                                 | <b>General Commands Manual</b><br><b>PAGESTUFF(1)</b> |
| <b>NAME</b>                                                                                                                                                                                                                                                                                                                                         |                                                       |
| pagestuff - Mach-O <b>file</b> page analysis tool                                                                                                                                                                                                                                                                                                   |                                                       |
| <b>SYNOPSIS</b>                                                                                                                                                                                                                                                                                                                                     |                                                       |
| pagestuff <b>file</b> [-a] [-p] [pagenumber...]                                                                                                                                                                                                                                                                                                     |                                                       |
| <b>DESCRIPTION</b>                                                                                                                                                                                                                                                                                                                                  |                                                       |
| <p>pagestuff displays information about the specified logical pages of a <b>file</b> conforming 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 <b>__TEXT</b>, <b>__text</b> section are displayed.</p> |                                                       |
| <p>The options to pagestuff(1) are:</p>                                                                                                                                                                                                                                                                                                             |                                                       |
| <p><b>-a</b> Displays all pages. All other arguments are ignored.</p>                                                                                                                                                                                                                                                                               |                                                       |
| <p><b>-p</b> Print a list of the sections of the specified Mach-O file, with offsets and lengths. All other arguments are ignored. Note that the size(1) tool given arguments "<b>-m -l -x</b>" displays a much more concise listing.</p>                                                                                                           |                                                       |
| <b>SEE ALSO</b>                                                                                                                                                                                                                                                                                                                                     |                                                       |
| <p><b>Mach-O(5)</b>, <b>size(1)</b></p>                                                                                                                                                                                                                                                                                                             |                                                       |
| Apple Computer, Inc.                                                                                                                                                                                                                                                                                                                                | January 3, 2001                                       |
| <b>PAGESTUFF(1)</b>                                                                                                                                                                                                                                                                                                                                 |                                                       |

## 附录

下面列出相关参考资料。

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2022-03-17 20:39:28

# 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 \(github.com\)](https://github.com/aidansteele/osx-abi-macho-file-format-reference/raw/master/Mach-O_File_Format.pdf)
        - [Mach-O\\_File\\_Format.pdf](#)
          - [https://github.com/aidansteele/osx-abi-macho-file-format-reference/raw/master/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 \(apple.com\)](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2023-10-06 16:50:17

## 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](http://apple.com))
- iOS/Mach\_and\_BSD.md at master · writeups/iOS · GitHub
- Mach-O - Wikipedia
- Introduction to Code Size Performance Guidelines ([apple.com](http://apple.com))
- aidansteele/osx-abi-macho-file-format-reference: Mirror of OS X ABI Mach-O File Format Reference ([github.com](https://github.com))
- Understanding the Mach-O File Format | by Travis Matthews | Medium
- Parsing Mach-O files - Low Level Bits
- Mach-O Executables · [objc.io](http://objc.io)
- The Mach-O binary file format - Mobile Application Penetration Testing [Book] ([oreilly.com](http://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](http://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](http://jianshu.com))
- Package Id - The Go Programming Language ([google.cn](http://google.cn))
- osx-abi-macho-file-format-reference/Mach-O\_File\_Format.pdf at master · aidansteele/osx-abi-macho-file-format-reference ([github.com](https://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](https://github.com))
- Overview of the Mach-O Executable Format ([apple.com](http://apple.com))
- Position-Independent Code
- Mach-O文件结构理解 | LJ小窝 ([jianli2017.top](http://jianli2017.top))
- Edgar's Blog ([tbfungeek.github.io](http://tbfungeek.github.io))
- Building Mach-O Files ([apple.com](http://apple.com))
- Crack prevention - iPhone Development Wiki
- iOS逆向---iOS11以后绕过越狱检测-CSDN博客
- 0xed/class-dump at swift-binaries ([github.com](https://github.com))
- Symbolicating iOS Crash Reports and Logs | Bugsnag Blog
- 求教otool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](http://newosxbook.com))

- MachO文件格式 ([liangmc.com](http://liangmc.com))
- Mach-O/README.md at master · XLsn0w/Mach-O ([github.com](https://github.com/XLsn0w/Mach-O))
- 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](https://github.com/XLsn0w/Mach-O))
- How to Reverse Engineer and Patch an iOS Application for Beginners: Part I ([inversecos.com](http://inversecos.com))
- pagestuff(1) [osx man page] ([unix.com](http://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](http://slideshare.net))
- macho.rs - source ([docs.rs](http://docs.rs))
- llilos/chained\_fixups.md at main · qyang-nj/llilos ([github.com](https://github.com/qyang-nj/llilos))
- llilos/README.md at main · qyang-nj/llilos ([github.com](https://github.com/qyang-nj/llilos))
- iOS逆向分析笔记 - 简书 ([jianshu.com](http://jianshu.com))
- iOS-Reverse/README.md at master · XLsn0w/iOS-Reverse ([github.com](https://github.com/XLsn0w/iOS-Reverse))
- [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](http://juejin.cn))
- Principle of Dynamic Linking of Imported Functions in Mach-O ([apriorit.com](http://apriorit.com))
- 图解 Mach-O 中的 got - 掘金 ([juejin.cn](http://juejin.cn))
- Understanding Concepts of VA, RVA and File Offsets ([tech-zealots.com](http://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
- 

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2023-10-07 22:17:52