

目录

前言	1.1
Swift逆向概览	1.2
Swift基础知识	1.3
Swift逆向相关	1.4
静态分析	1.4.1
导出头文件	1.4.1.1
IDA分析	1.4.1.2
动态调试	1.4.2
Swift通用逻辑	1.5
TypeMetadata	1.5.1
ValueMetadata	1.5.1.1
VWT	1.5.1.1.1
StructMetadata	1.5.1.1.2
ClassMetadata	1.5.1.2
内存布局	1.5.1.2.1
图	1.5.1.2.1.1
文字	1.5.1.2.1.2
Swift源码	1.5.1.2.1.3
IDA定义	1.5.1.2.1.4
举例	1.5.1.2.1.5
MetadataKind	1.5.2
ValueBuffer	1.5.3
常用类型	1.6
String字符串	1.6.1
内存布局	1.6.1.1
图	1.6.1.1.1
文字	1.6.1.1.2
Swift源码	1.6.1.1.3
IDA定义	1.6.1.1.4
举例	1.6.1.1.5
Array数组	1.6.2
内存布局	1.6.2.1
图	1.6.2.1.1
文字	1.6.2.1.2

Swift源码	1.6.2.1.3
IDA定义	1.6.2.1.4
举例	1.6.2.1.5
Set集合	1.6.3
内存布局	1.6.3.1
图	1.6.3.1.1
文字	1.6.3.1.2
Swift源码	1.6.3.1.3
IDA定义	1.6.3.1.4
举例	1.6.3.1.5
Dictionary字典	1.6.4
内存布局	1.6.4.1
图	1.6.4.1.1
文字	1.6.4.1.2
Swift源码	1.6.4.1.3
IDA定义	1.6.4.1.4
举例	1.6.4.1.5
Data数据	1.6.5
内存布局	1.6.5.1
图	1.6.5.1.1
文字	1.6.5.1.2
Swift源码	1.6.5.1.3
IDA定义	1.6.5.1.4
举例	1.6.5.1.5
Struct结构体	1.6.6
内存布局	1.6.6.1
图	1.6.6.1.1
文字	1.6.6.1.2
Swift源码	1.6.6.1.3
IDA定义	1.6.6.1.4
举例	1.6.6.1.5
Bool布尔	1.6.7
Enum枚举	1.6.8
Tuple元祖	1.6.9
Int整型	1.6.10
附录	1.7
参考资料	1.7.1

iOS逆向：Swift逆向

- 最新版本: v0.8
- 更新时间: 20240224

简介

整理iOS逆向期间，关于Swift逆向相关的各种知识。包括通用逻辑和各种常见类型，尤其是各种类型的内存布局。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

HonKit源码

- [crifan/ios_re_swift_reverse: iOS逆向：Swift逆向](#)

如何使用此HonKit源码去生成发布为电子书

详见：[crifan/honkit_template: demo how to use crifan honkit template and demo](#)

在线浏览

- [iOS逆向：Swift逆向 book.crifan.org](#)
- [iOS逆向：Swift逆向 crifan.github.io](#)

离线下载阅读

- [iOS逆向：Swift逆向 PDF](#)
- [iOS逆向：Swift逆向 ePUB](#)
- [iOS逆向：Swift逆向 Mobi](#)

版权和用途说明

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

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

鸣谢

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

其他

作者的其他电子书

本人 crifan 还写了其他 150+ 本电子书教程，感兴趣可移步至：

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

关于作者

关于作者更多介绍，详见：

[关于CrifanLi李茂 – 在路上](#)

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：

2024-02-24 16:19:21

Swift逆向概览

iOS逆向期间，有些app二进制代码内部是：objc 和Swift混合的。

所以涉及到：Swift逆向。

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：
2024-02-22 09:31:07

Swift基础知识

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：
2024-02-22 09:35:44

Swift逆向相关

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：
2024-02-22 09:28:48

Swift逆向之静态分析

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：
2024-02-22 09:27:31

导出Swift头文件

TODO: 把导出ObjC和Swift混淆时会报错的问题，和解决办法（最新版的class-dump），整理过来

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：
2024-02-22 09:29:18

IDA分析Swift

TODO: 把已加到IDA中的，各种类型的定义，整理过来

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：
2024-02-22 09:30:57

Swift逆向之动态调试

调试时，辅助用IDA打开Swift的各种库文件，比如：

- libswiftCore.dylib
- libswiftFoundation.dylib
- 等等

方便调试内容。

这样，通过动态调试和查看IDA中的分析，函数的伪代码实现等等，就可以有更深入的理解很多函数和变量了。

TODO：把下面帖子中有用的内容，整理过来：

- 【未解决】iOS逆向Swift: swift_getAssociatedTypeWitness
- 【未解决】iOS逆向Swift: Data.withUnsafeMutableBytes(_:)
- 【已解决】iOS逆向Swift: Data.withUnsafeBytes(_:)
- 【未解决】iOS逆向WhatsApp: swiftPodCopy_10039A1B4
- 【未解决】iOS逆向Swift: Set.init(_:)
-
- 【记录】iOS逆向Swift: IDA静态分析libswiftFoundation.dylib
 - . . .
- 【已解决】iOS逆向Swift: 库文件libswiftCore.dylib
 - 【已解决】iOS逆向WhatsApp: ArrayAdoptStorage_2ToW1_CB2C
 - static Swift.Array.adoptStorage(: __owned Swift._ContiguousArrayStorage<T_0_0>, count: Swift.Int) -> (Swift.Array<T_0_0>, Swift.UnsafeMutablePointer<T_0_0>)
 - 【已解决】iOS逆向: dyld_stub_binder
 - 【已解决】iOS逆向Swift: String的WitnessTable详情
 - destroy value witness for Swift.String
 - 【已解决】iOS逆向Swift: Float对应的Builtin.Int32的VWT的具体值
 - type metadata for Swift.Float
 - 【未解决】iOS逆向Swift: _NativeSet._unsafeInsertNew
 - Swift.NativeSet._unsafeInsertNew(: __owned T_0_0, at: Swift._HashTable.Bucket) -> ()
 - 【已解决】iOS逆向Swift: Optional的VWT=ValueWitnessTable
 - 【未解决】iOS逆向Swift: _SetStorage.allocate
 - static Swift._SetStorage.allocate(capacity: Swift.Int) -> Swift._SetStorage<T_0_0>
 - 【已解决】iOS逆向Swift: Xcode中给Swift函数_NativeSet.init加断点
 - Swift._NativeSet.init(capacity: Swift.Int) -> Swift._NativeSet<T_0_0>
 - 【未解决】iOS逆向Swift: NativeSet
 - Collection
 - 【未解决】iOS逆向WhatsApp: Collection.map(_:) (void)
 - 【未解决】iOS逆向Swift: swift_getAssociatedTypeWitness
 - Swift.Collection.isEmpty.getter : Swift.Bool

- 【基本解决】iOS逆向Swift: protocol requirements base descriptor的含义
 - protocol requirements base descriptor for Swift.Collection
 - 【已解决】iOS逆向: Swift.pod_copy
 - pod_copy(swift::OpaqueValue, swift::OpaqueValue, swift::TargetMetadata<_inprocess class="copyright"> const*)
 - 【已解决】iOS逆向: Swift._ContiguousArrayStorage
 - type metadata accessor for Swift._ContiguousArrayStorage
 - 【已解决】iOS逆向: swift_getTypeByMangledNameInContext
 - 【未解决】iOS逆向: __swift_instantiateConcreteTypeFromMangledName
 - 【已解决】iOS逆向WhatsApp: Swift函数String.append(_:)的字符串拼接的实现逻辑
 - Swift.String.append(Swift.String) -> ()
-

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:
2024-02-22 09:34:33

Swift通用逻辑

- 其他
 - ValueBuffer
 - Existential Container?
 - Box?
 - Opaque ?

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：
2024-02-22 09:32:50

TypeMetadata

- Swift中有几种Metadata
 - 主要有2类
 - Class的: TargetClassMetadata == ClassMetadata
 - 非Class的= (Struct、Enum、Optional等) Value的: TargetValueMetadata = ValueMetadata
 - 通用逻辑
 - TargetClassMetadata和TargetValueMetadata, 都继承自: TargetMetadata
 - TargetMetadata
 - 属性=字段
 - Kind 另外一种表述:
- Swift中的 Metadata
 - TargetMetadata
 - ClassMetadata
 - == TargetClassMetadata
 - 适用于: **Class**类
 - ValueMetadata
 - == TargetValueMetadata
 - 适用于: **非Class** == Struct 、 Enum 、 Optional 等**Value**

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:
2024-02-22 10:22:10

ValueMetadata

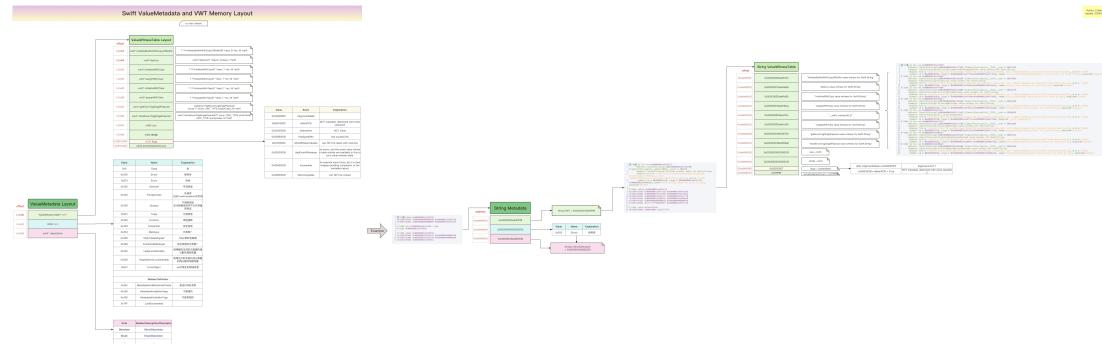
内存布局

图

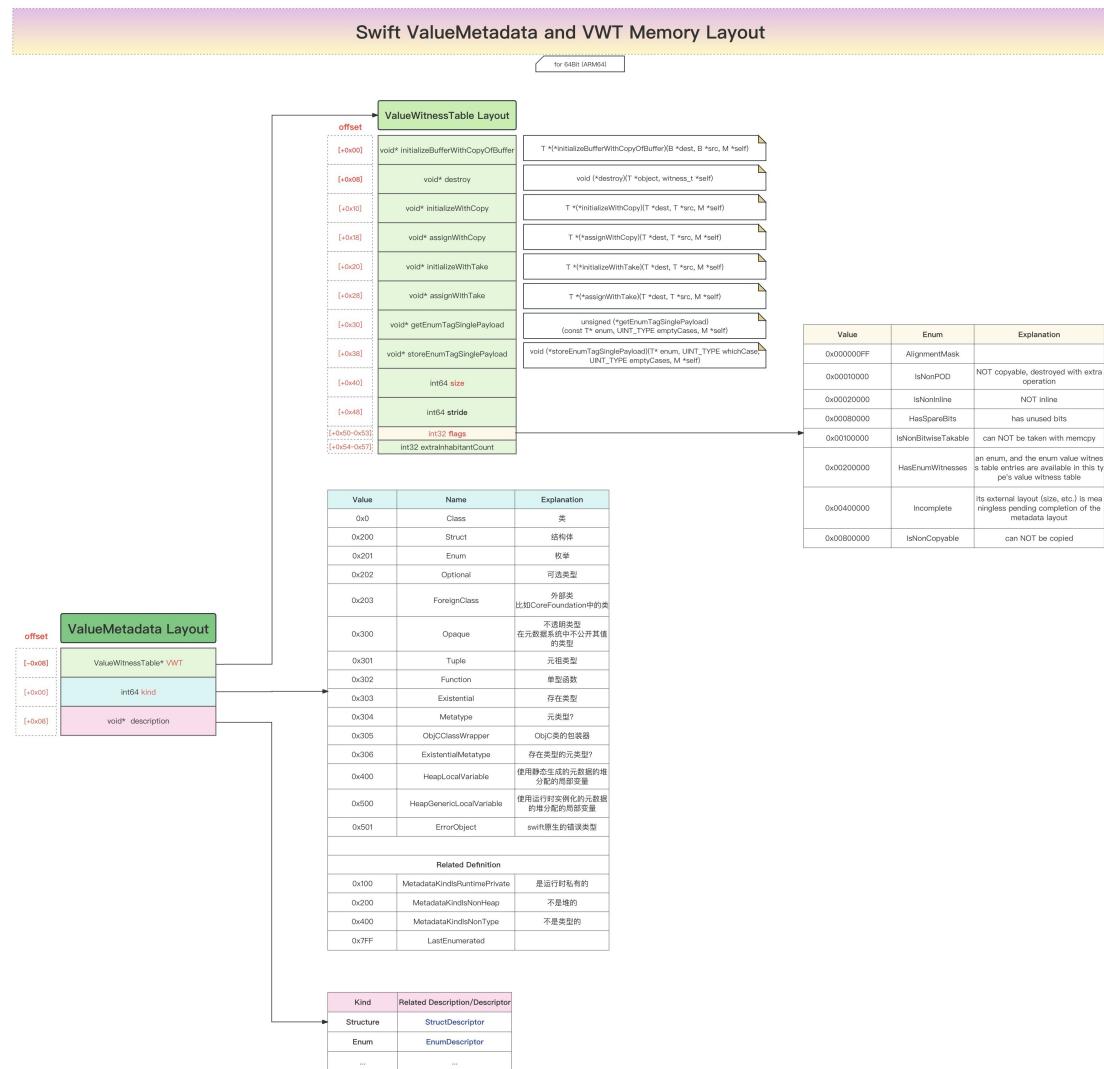
- Swift的ValueMetadata和VWT的内存布局结构图 = Swift ValueMetadata and VWT Memory Layout
 - 在线预览

▪ [Swift的ValueMetadata和VWT的内存布局结构图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)

- 离线查看



- 核心定义



文字

- Swift中的：TargetValueMetadata
 - 继承关系
 - TargetValueMetadata = ValueMetadata
 - TargetMetadata
 - 字段=属性=内存布局
 - TargetMetadata
 - StoredPointer Kind
 - the kind. Only valid for non-class metadata; getKind() must be used to get the kind value
 - TargetValueMetadata
 - TargetSignedPointer* Description
 - An out-of-line description of the type
 - 说明
 - 此处的Description根据具体类型不同，则是不同的内容
 - 举例
 - Struct
 - TargetStructDescriptor=StructDescriptor

加到IDA中的定义

```
struct ValueMetadata
{
    __int64 kind;
    void description;
};
```

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:
2024-02-23 14:44:48

VWT = ValueWitnessTable

概述

VWT结构布局

文字

- Swift 的 VWT = Value Witness Table 结构布局=字段=属性
 - [+0x00] = void* initializeBufferWithCopyOfBuffer
 - [+0x08] = void* destroy
 - [+0x10] = void* initializeWithCopy
 - [+0x18] = void* assignWithCopy
 - [+0x20] = void* initializeWithTake
 - [+0x28] = void* assignWithTake
 - [+0x30] = void* getEnumTagSinglePayload
 - [+0x38] = void* storeEnumTagSinglePayload
 - [+0x40] = void* int64 size
 - [+0x48] = void* int64 stride
 - [+0x50~0x53] = int32 flags
 - [+0x54~0x57] = int32 extraInhabitantCount

图

详见：

[ValueMetadata](#)

加入到IDA中的定义

- struct ValueWitnessTable

```
struct __cppobj ValueWitnessTable
{
    void (__fastcall *initializeBufferWithCopyOfBuffer)(void *dst, void *src, void *metadataSelf);
    void (__fastcall *destroy)(void *object, void *witnessSelf);
    void (__fastcall *initializeWithCopy)(void *dst, void *src, void *metadataSelf);
    void (__fastcall *assignWithCopy)(void *dst, void *src, void *metadataSelf);
    void (__fastcall *initializeWithTake)(void *dst, void *src, void *metadataSelf);
    void (__fastcall *assignWithTake)(void *dst, void *src, void *metadataSelf);
    unsigned __int64 (__fastcall *getEnumTagSinglePayload)(void *enumPtr, __int64 emptyCases, void *metadataSelf);
    void (__fastcall *storeEnumTagSinglePayload)(void *enumPtr, __int64 whichCase, void *metadataSelf);
    __int64 size;
    __int64 stride;
```

```
    TargetValueWitnessFlags flags;
    __int32 extraInhabitantCount;
};
```

- enum TargetValueWitnessFlags

```
000000FF ; enum TargetValueWitnessFlags, mappedto_10385, bitfield, width 4 bytes
000000FF AlignmentMask     EQU 0xFF
00010000 IsNonPOD        EQU 0x10000
00020000 IsNonInline      EQU 0x20000
00080000 HasSpareBits    EQU 0x80000
00100000 IsNonBitwiseTakable EQU 0x100000
00200000 HasEnumWitnesses EQU 0x200000
00400000 Incomplete       EQU 0x400000
00800000 IsNonCopyable    EQU 0x800000
00800000
```

详解

内存布局

- Swift 的 VWT = Value Witness Table 结构布局=字段=属性
 - [+0x00] = initializeBufferWithCopyOfBuffer
 - 定义: `T *(*initializeBufferWithCopyOfBuffer)(B *dest, B *src, M *self);`
 - [+0x08] = destroy
 - 定义: `void (*destroy)(T *object, witness_t *self);`
 - [+0x10] = initializeWithCopy
 - 定义: `T *(*initializeWithCopy)(T *dest, T *src, M *self);`
 - [+0x18] = assignWithCopy
 - 定义: `T *(*assignWithCopy)(T *dest, T *src, M *self);`
 - [+0x20] = initializeWithTake
 - 定义: `T *(*initializeWithTake)(T *dest, T *src, M *self);`
 - [+0x28] = assignWithTake
 - 定义: `T *(*assignWithTake)(T *dest, T *src, M *self);`
 - [+0x30] = getEnumTagSinglePayload
 - 定义: `unsigned (*getEnumTagSinglePayload)(const T* enum, UINT_TYPE emptyCases, M *self);`
 - [+0x38] = storeEnumTagSinglePayload
 - 定义: `void (*storeEnumTagSinglePayload)(T* enum, UINT_TYPE whichCase, UINT_TYPE emptyCases, M *self);`
 - [+0x40] = size
 - 定义: `SIZE_TYPE size;`
 - [+0x48] = stride
 - 定义: `SIZE_TYPE stride;`
 - [+0x50~0x53] = flags
 - 定义: `UINT_TYPE flags;`

- [+0x54~0x57] = extraInhabitantCount
 - 定义: `UINT_TYPE extraInhabitantCount;`
- 说明
 - `SIZE_TYPE = StoredSize = size_t ? = int64`
 - `UINT_TYPE = unsigned = int32`

Swift代码

[swift-language/include/swift/ABI/ValueWitness.def at master · eplataniots/swift-language](https://github.com/eplataniots/swift-language/blob/master/swift/include/swift/ABI/ValueWitness.def)

```

/// T *(*initializeBufferWithCopyOfBuffer)(B *dest, B *src, M *self);
/// Given an invalid buffer, initialize it as a copy of the
/// object in the source buffer.
FUNCTION_VALUE_WITNESS(initializeBufferWithCopyOfBuffer,
                      InitializeBufferWithCopyOfBuffer,
                      MUTABLE_VALUE_TYPE,
                      (MUTABLE_BUFFER_TYPE, MUTABLE_BUFFER_TYPE, TYPE_TYPE))

BEGIN_VALUE_WITNESS_RANGE(ValueWitness,
                           InitializeBufferWithCopyOfBuffer)
BEGIN_VALUE_WITNESS_RANGE(RequiredValueWitness,
                           InitializeBufferWithCopyOfBuffer)
BEGIN_VALUE_WITNESS_RANGE(RequiredValueWitnessFunction,
                           InitializeBufferWithCopyOfBuffer)

/// void (*destroy)(T *object, witness_t *self);
///
/// Given a valid object of this type, destroy it, leaving it as an
/// invalid object. This is useful when generically destroying
/// an object which has been allocated in-line, such as an array,
/// struct, or tuple element.
FUNCTION_VALUE_WITNESS(destroy,
                      Destroy,
                      VOID_TYPE,
                      (MUTABLE_VALUE_TYPE, TYPE_TYPE))

/// T *(*initializeWithCopy)(T *dest, T *src, M *self);
///
/// Given an invalid object of this type, initialize it as a copy of
/// the source object. Returns the dest object.
FUNCTION_VALUE_WITNESS(initializeWithCopy,
                      InitializeWithCopy,
                      MUTABLE_VALUE_TYPE,
                      (MUTABLE_VALUE_TYPE, MUTABLE_VALUE_TYPE, TYPE_TYPE))

/// T *(*assignWithCopy)(T *dest, T *src, M *self);
///
/// Given a valid object of this type, change it to be a copy of the
/// source object. Returns the dest object.
FUNCTION_VALUE_WITNESS(assignWithCopy,
                      AssignWithCopy,
                      MUTABLE_VALUE_TYPE,
                      (MUTABLE_VALUE_TYPE, MUTABLE_VALUE_TYPE, TYPE_TYPE))

```

```

    /// T *(*initializeWithTake)(T *dest, T *src, M *self);
    ///
    /// Given an invalid object of this type, initialize it by taking
    /// the value of the source object. The source object becomes
    /// invalid. Returns the dest object.
FUNCTION_VALUE_WITNESS(initializeWithTake,
    InitializeWithTake,
    MUTABLE_VALUE_TYPE,
    (MUTABLE_VALUE_TYPE, MUTABLE_VALUE_TYPE, TYPE_TYPE))

    /// T *(*assignWithTake)(T *dest, T *src, M *self);
    ///
    /// Given a valid object of this type, change it to be a copy of the
    /// source object. The source object becomes invalid. Returns the
    /// dest object.
FUNCTION_VALUE_WITNESS(assignWithTake,
    AssignWithTake,
    MUTABLE_VALUE_TYPE,
    (MUTABLE_VALUE_TYPE, MUTABLE_VALUE_TYPE, TYPE_TYPE))

    /// unsigned (*getEnumTagSinglePayload)(const T* enum, UINT_TYPE emptyCases)
    /// Given an instance of valid single payload enum with a payload of this
    /// witness table's type (e.g Optional<ThisType>), get the tag of the enum.
FUNCTION_VALUE_WITNESS(getEnumTagSinglePayload,
    GetEnumTagSinglePayload,
    UINT_TYPE,
    (IMMUTABLE_VALUE_TYPE, UINT_TYPE, TYPE_TYPE))

    /// void (*storeEnumTagSinglePayload)(T* enum, UINT_TYPE whichCase,
    ///                                     UINT_TYPE emptyCases)
    /// Given uninitialized memory for an instance of a single payload enum with a
    /// payload of this witness table's type (e.g Optional<ThisType>), store the
    /// tag.
FUNCTION_VALUE_WITNESS(storeEnumTagSinglePayload,
    StoreEnumTagSinglePayload,
    VOID_TYPE,
    (MUTABLE_VALUE_TYPE, UINT_TYPE, UINT_TYPE, TYPE_TYPE))

END_VALUE_WITNESS_RANGE(RequiredValueWitnessFunction,
    StoreEnumTagSinglePayload)

    /// SIZE_TYPE size;
    ///
    /// The required storage size of a single object of this type.
DATA_VALUE_WITNESS(size,
    Size,
    SIZE_TYPE)

BEGIN_VALUE_WITNESS_RANGE(TypeLayoutWitness,
    Size)

BEGIN_VALUE_WITNESS_RANGE(RequiredTypeLayoutWitness,
    Size)

    /// SIZE_TYPE stride;
    ///

```

```

/// The required size per element of an array of this type. It is at least
/// one, even for zero-sized types, like the empty tuple.
DATA_VALUE_WITNESS(stride,
                     Stride,
                     SIZE_TYPE)

///     UINT_TYPE flags;
///
/// The ValueWitnessAlignmentMask bits represent the required
/// alignment of the first byte of an object of this type, expressed
/// as a mask of the low bits that must not be set in the pointer.
/// This representation can be easily converted to the 'alignof'
/// result by merely adding 1, but it is more directly useful for
/// performing dynamic structure layouts, and it grants an
/// additional bit of precision in a compact field without needing
/// to switch to an exponent representation.
///
/// The ValueWitnessIsNonPOD bit is set if the type is not POD.
///
/// The ValueWitnessIsNonInline bit is set if the type cannot be
/// represented in a fixed-size buffer or if it is not bitwise takable.
///
/// The ExtraInhabitantsMask bits represent the number of "extra inhabitants"
/// of the bit representation of the value that do not form valid values of
/// the type.
///
/// The Enum_HasSpareBits bit is set if the type's binary representation
/// has unused bits.
///
/// The HasEnumWitnesses bit is set if the type is an enum type.
DATA_VALUE_WITNESS(flags,
                    Flags,
                    UINT_TYPE)

///     UINT_TYPE extraInhabitantCount;
///
/// The number of extra inhabitants in the type.
DATA_VALUE_WITNESS(extraInhabitantCount,
                    ExtraInhabitantCount,
                    UINT_TYPE)

END_VALUE_WITNESS_RANGE(RequiredTypeLayoutWitness,
                        ExtraInhabitantCount)

END_VALUE_WITNESS_RANGE(RequiredValueWitness,
                        ExtraInhabitantCount)

END_VALUE_WITNESS_RANGE(TypeLayoutWitness,
                        ExtraInhabitantCount)

#endif /* WANT_REQUIRED_VALUE_WITNESSES */

#if WANT_ENUM_VALUE_WITNESSES

// The following value witnesses are conditionally present if the witnessed

```

```

// type is an enum.

/// unsigned (*getEnumTag)(T *obj, M *self);
///

/// Given a valid object of this enum type, extracts the tag value indicating
/// which case of the enum is inhabited. Returned values are in the range
/// [0..NumElements-1].
FUNCTION_VALUE_WITNESS(getEnumTag,
    GetEnumTag,
    INT_TYPE,
    (IMMUTABLE_VALUE_TYPE, TYPE_TYPE))

BEGIN_VALUE_WITNESS_RANGE(EnumValueWitness,
    GetEnumTag)

/// void (*destructiveProjectEnumData)(T *obj, M *self);
/// Given a valid object of this enum type, destructively extracts the
/// associated payload.
FUNCTION_VALUE_WITNESS(destructiveProjectEnumData,
    DestructiveProjectEnumData,
    VOID_TYPE,
    (MUTABLE_VALUE_TYPE, TYPE_TYPE))

/// void (*destructiveInjectEnumTag)(T *obj, unsigned tag, M *self);
/// Given an enum case tag and a valid object of case's payload type,
/// destructively inserts the tag into the payload. The given tag value
/// must be in the range [-ElementsWithPayload..ElementsWithNoPayload-1].
FUNCTION_VALUE_WITNESS(destructiveInjectEnumTag,
    DestructiveInjectEnumTag,
    VOID_TYPE,
    (MUTABLE_VALUE_TYPE, UINT_TYPE, TYPE_TYPE))

END_VALUE_WITNESS_RANGE(EnumValueWitness,
    DestructiveInjectEnumTag)

END_VALUE_WITNESS_RANGE(ValueWitness,
    DestructiveInjectEnumTag)

```

Swift的VWT和C++对应关系

Swift Value Witness Operation	C++ equivalent
initializeWithCopy	copy constructor
assignWithCopy	copy assignment operator
initializeWithTake	move constructor, followed by a call to destructor on the source
assignWithTake	move assignment operator, followed by a call to destructor on the source
destroy	destructor
size	sizeof(T) minus trailing padding
stride	sizeof(T)

flags among other information, contains alignment, i.e., `alignof(T)`

举例

Builtin.NativeObject的VWT

- Builtin.NativeObject的VWT内存布局
 - [+0x00] = initializeBufferWithCopyOfBuffer
 - name="swift::metadataimpl::BufferValueWitnesses< :metadataimpl::SwiftRetainableBox>, true, 8ul, 8ul, (swift::metadataimpl::FixedPacking)1>::initializeBufferWithCopyOfBuffer(swift::TargetValueBuffer< :InProcess>*, swift::TargetValueBuffer< :InProcess>*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl20BufferValueWitnessesINS0_14ValueWitnessesINS0_18SwiftRetainableBoxEEELb1ELm8ELm8ELNS0_12FixedPackingE1EE32initializeBufferWithCopyOfBufferEPNS_17TargetValueBufferINS_9InProcessEEESA_PKNS_14TargetMetadataIS8_EE"
 - [+0x08] = destroy
 - name="swift::metadataimpl::ValueWitnesses< :metadataimpl::SwiftRetainableBox>::destroy(swift::OpaqueValue*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE7destroyEPNS_110opaqueValueEPKNS_14TargetMetadataINS_9InProcessEEE"
 - [+0x10] = initializeWithCopy
 - name="swift::metadataimpl::ValueWitnesses< :metadataimpl::SwiftRetainableBox>::initializeWithCopy(swift::OpaqueValue*, swift::OpaqueValue*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE18initializeWithCopyEPNS_110opaqueValueES5_PKNS_14TargetMetadataINS_9InProcessEEE"
 - [+0x18] = assignWithCopy
 - name="swift::metadataimpl::ValueWitnesses< :metadataimpl::SwiftRetainableBox>::assignWithCopy(swift::OpaqueValue*, swift::OpaqueValue*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE14assignWithCopyEPNS_110opaqueValueES5_PKNS_14TargetMetadataINS_9InProcessEEE"
 - [+0x20] = initializeWithTake
 - name="swift::metadataimpl::ValueWitnesses< :metadataimpl::SwiftRetainableBox>::initializeWithTake(swift::OpaqueValue*, swift::OpaqueValue*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE18initializeWithTakeEPNS_110opaqueValueES5_PKNS_14TargetMetadataINS_9InProcessEEE"
 - [+0x28] = assignWithTake
 - name="swift::metadataimpl::ValueWitnesses< :metadataimpl::SwiftRetainableBox>::assignWithTake(swift::OpaqueValue*, swift::OpaqueValue*, swift::TargetMetadata< :InProcess> const*)"
 - mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE14assignWithTakeEPNS_110opaqueValueES5_PKNS_14TargetMetadataINS_9InProcessEEE"

- ```
Box>::assignWithTake(swift::OpaqueValue*, swift::OpaqueValue*,
swift::TargetMetadata< :InProcess> const*)"
■ mangled="_ZN5swift12metadataimpl14ValueWitnessesINS0_18SwiftRetainableBoxEE
14assignWithTakeEPNS_110opaqueValueES5_PKNS_14TargetMetadataINS_9InProcessEEE

○ [+0x30] = getEnumTagSinglePayload
■ name="swift::metadataimpl::FixedSizeBufferValueWitnesses<swift::metadataimpl::
ValueWitnesses< :metadataimpl::SwiftRetainableBox>, true, 8ul, 8ul,
true>::getEnumTagSinglePayload(swift::OpaqueValue const*, unsigned int,
swift::TargetMetadata< :InProcess> const*)"
■ mangled="_ZN5swift12metadataimpl29FixedSizeBufferValueWitnessesINS0_14Value
WitnessesINS0_18SwiftRetainableBoxEEELb1ELm8ELm8ELb1EE23getEnumTagSinglePayl
oadEPKNS_110opaqueValueEjPKNS_14TargetMetadataINS_9InProcessEEE"

○ [+0x38] = storeEnumTagSinglePayload
■ name="swift::metadataimpl::FixedSizeBufferValueWitnesses<swift::metadataimpl::
ValueWitnesses< :metadataimpl::SwiftRetainableBox>, true, 8ul, 8ul,
true>::storeEnumTagSinglePayload(swift::OpaqueValue*, unsigned int, unsigned
int, swift::TargetMetadata< :InProcess> const*)"
■ mangled="_ZN5swift12metadataimpl29FixedSizeBufferValueWitnessesINS0_14Value
WitnessesINS0_18SwiftRetainableBoxEEELb1ELm8ELm8ELb1EE25storeEnumTagSinglePa
yloadEPNS_110opaqueValueEjjPKNS_14TargetMetadataINS_9InProcessEEE"

○ [+0x40] = int64 size
■ 0x0000000000000008

○ [+0x48] = int64 stride
■ 0x0000000000000008

○ [+0x50~0x53] = int32 flags
■ 0x00010007

○ [+0x54~0x57] = int32 extraInhabitantCount
■ 0x7fffffff
```

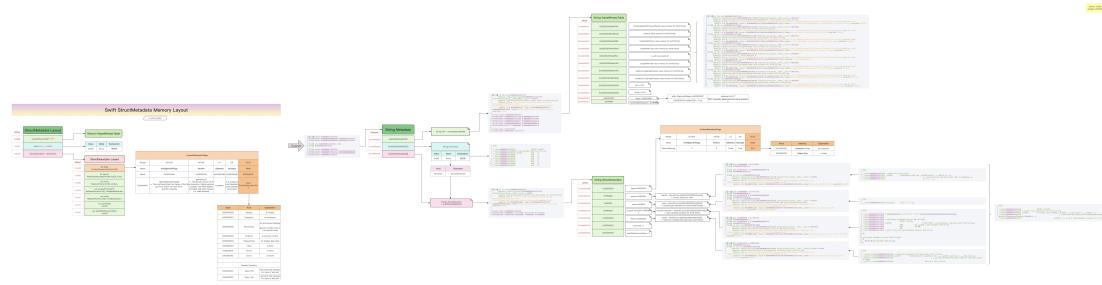
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新:  
2024-02-23 14:50:55

# StructMetadata

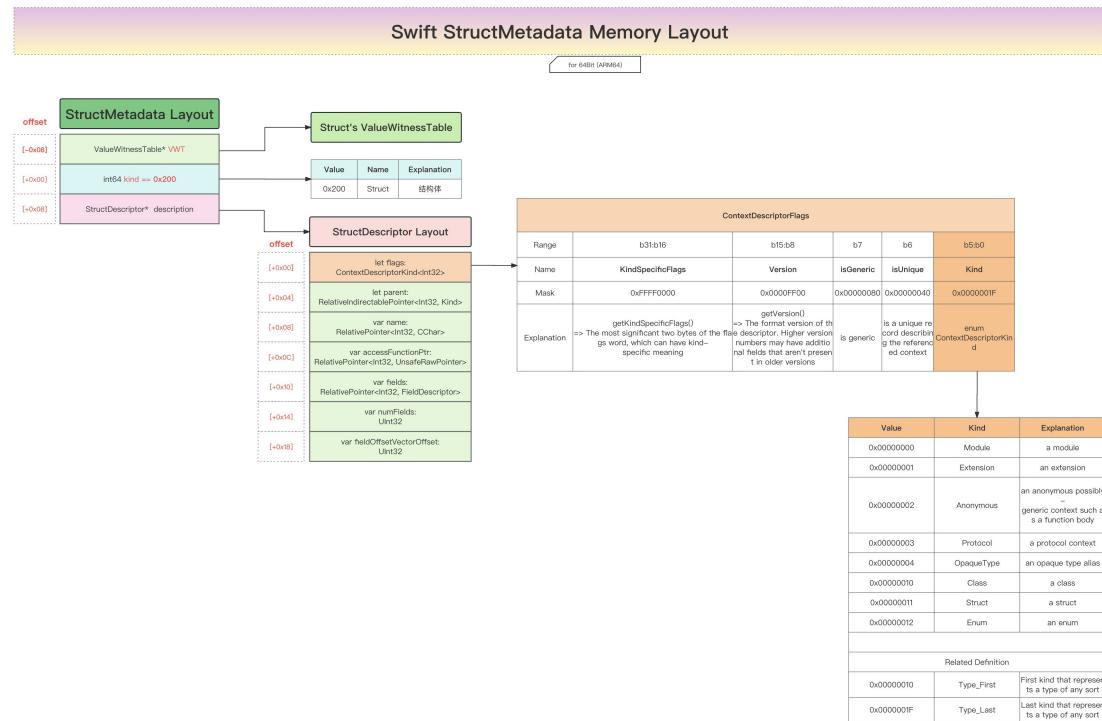
## StructMetadata的内存布局

### 图

- Swift的StructMetadata内存布局图 = Swift ValueMetadata Memory Layout
  - 在线预览
    - [Swift的StructMetadata内存布局图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)
  - 离线查看



- 核心定义



### 文字

- Swift的StructMetadata的内存布局
  - [-0x08] = ValueWitnessTable\* vwt;
  - [+0x00] = int64 kind // 是固定的: 0x200
  - [+0x08] = StructDescriptor\* description
    - StructDescriptor
      - FieldDescriptor

- FieldRecord

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:  
2024-02-23 14:55:08

# ClassMetadata

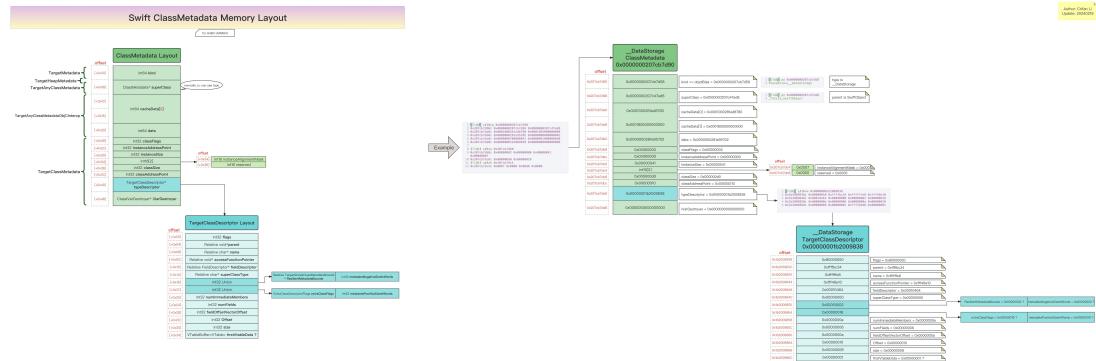
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:47:20

# 内存布局

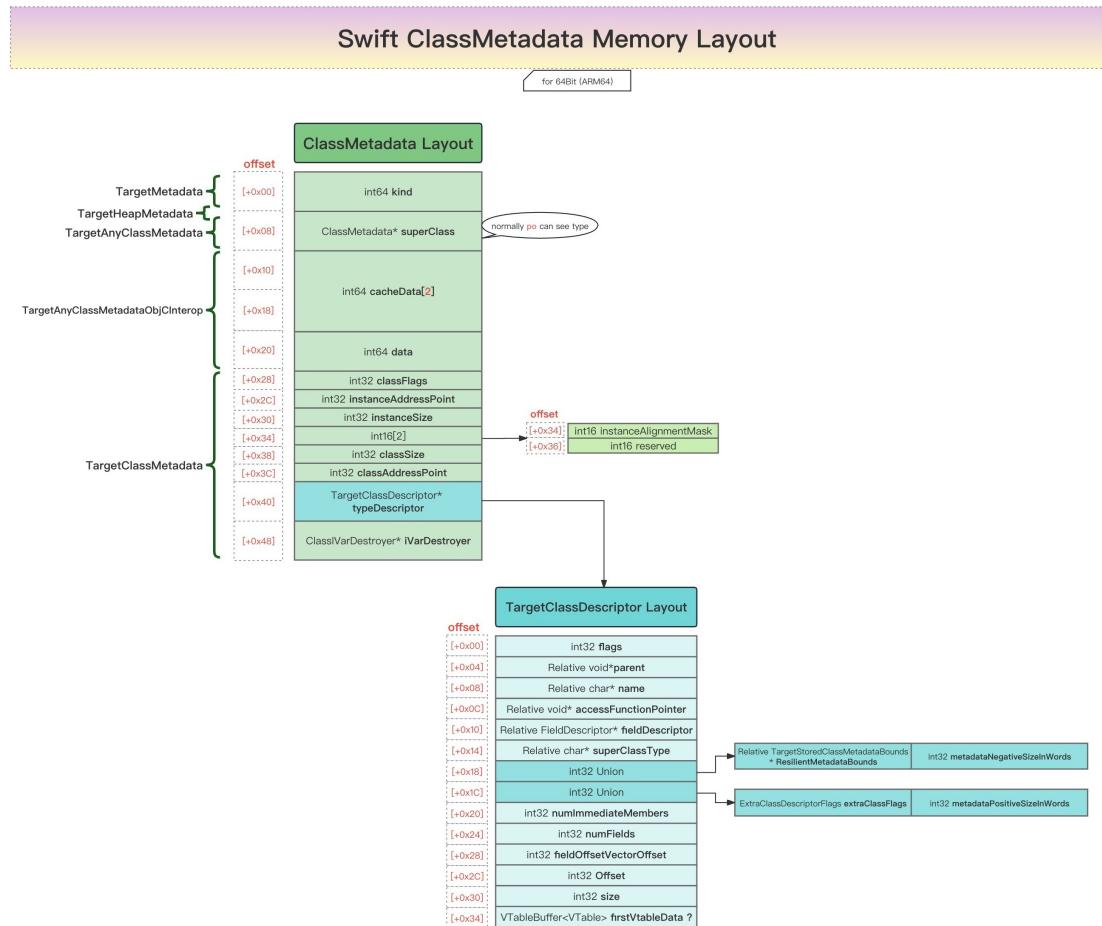
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:33:30

# Swift的ClassMetadata的内存布局结构图

- Swift的ClassMetadata的内存布局结构图 = Swift ClassMetadata Memory Layout
  - 在线预览
    - [Swift的ClassMetadata内存布局结构图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)
  - 离线查看



- 核心定义



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: 2024-02-22 09:48:50

# ClassMetadata的内存布局

## 概述

### ClassMetadata = Class的TypeMetadata

- Class的TypeMetadata
  - [+0x00] = var kind: Int
  - [+0x08] = var superClass: UnsafeMutablePointer
  - [+0x10] = Int cacheData[2]
  - [+0x20] = var data: Int
  - [+0x28] = var classFlags: Int32
  - [+0x2C] = var instanceAddressPoint: UInt32
  - [+0x30] = var instanceSize: UInt32
  - [+0x34] = var instanceAlignmentMask: UInt16
  - [+0x36] = var reserved: UInt16
  - [+0x38] = var classSize: UInt32
  - [+0x3C] = var classAddressPoint: UInt32
  - [+0x40] = var typeDescriptor: UnsafeMutablePointer
  - [+0x48] = var iVarDestroyer: UnsafeMutablePointer

## struct TargetClassDescriptor

- struct TargetClassDescriptor
  - [+0x00] = var flags: UInt32
  - [+0x04] = var parent: TargetRelativeDirectPointer
  - [+0x08] = var name: TargetRelativeDirectPointer
  - [+0x0C] = var accessFunctionPointer: TargetRelativeDirectPointer
  - [+0x10] = var fieldDescriptor: TargetRelativeDirectPointer
  - [+0x14] = var superClassType: TargetRelativeDirectPointer
  - [+0x18] = Int32 Union
    - var ResilientMetadataBounds: RelativeDirectPointer
    - var metadataNegativeSizeInWords: UInt32
  - [+0x1C] = Int32 Union
    - var extraClassFlags: ExtraClassDescriptorFlags
    - var metadataPositiveSizeInWords: UInt32
  - [+0x20] = var numImmediateMembers: UInt32
  - [+0x24] = var numFields: UInt32
  - [+0x28] = var fieldOffsetVectorOffset: UInt32
  - [+0x2C] = var Offset: UInt32
  - [+0x30] = var size: UInt32
  - [+0x34] = var firstVtableData: VTableBuffer

## 详解

### Swift中类的继承关系

- Swift中类的继承关系
  - 详解
    - TargetClassMetadataType == ClassMetadata
      - = TargetClassMetadata>
    - TargetClassMetadataObjCInterop
      - = TargetClassMetadata>
    - ->
    - TargetAnyClassMetadataType
      - ObjCInterop=true == 兼容ObjC类 == 支持Objective-C类互操作
        - TargetAnyClassMetadataObjCInterop
      - ObjCInterop=false == 不兼容ObjC类
        - TargetAnyClassMetadata
    - TargetAnyClassMetadataObjCInterop
      - TargetAnyClassMetadata
    - TargetClassMetadata
      - TargetAnyClassMetadataVariant
    - ->
    - TargetAnyClassMetadata
      - TargetHeapMetadata == HeapMetadata
        - TargetMetadata
- 概述
  - ClassMetadata
    - TargetClassMetadata
      - TargetAnyClassMetadataObjCInterop
        - TargetAnyClassMetadata
          - TargetHeapMetadata
            - TargetMetadata

### Swift中的： ClassMetadata 字段定义

- Swift中的： ClassMetadata 字段定义
  - TargetMetadata
    - var kind: Int
      - 在oc中放的就是isa, 在swift中kind大于0x7FF表示的就是类
  - TargetHeapMetadata
    - 没属性=字段
  - TargetAnyClassMetadata
    - var superClass: UnsafeMutablePointer<AnyClass>
      - 父类的Metadata, 如果是null说明是最顶级的root类了
  - TargetAnyClassMetadataObjCInterop
    - Int cacheData[2]
      - 缓存数据用于某些动态查找, 它由运行时拥有, 通常需要与Objective-C的使用进行互操

作。(说到底就是OC的东西)

- var data: Int
  - 除了编译器设置低位以表明这是Swift元类型(因此存在对应的类型元数据的头信息)外,这个data里存的指针,用于行外元数据,通常是不透明的(应该也是OC的)
- TargetClassMetadata
  - var classFlags: UInt32
    - Swift-specific class flags
  - var instanceAddressPoint: UInt32
    - The address point of instances of this type
  - var instanceSize: UInt32
    - The required size of instances of this type.(实例对象在堆内存的大小)
  - var instanceAlignmentMask: UInt16
    - The alignment mask of the address point of instances of this type. (根据这个mask来获取内存中的对齐大小)
  - var reserved: UInt16
    - Reserved for runtime use. (预留给运行时使用)
  - var classSize: UInt32
    - The total size of the class object, including prefix and suffix extents.
  - var classAddressPoint: UInt32
    - The offset of the address point within the class object.
  - var typeDescriptor: UnsafeMutablePointer
    - 一个对类型的超行的swift特定描述,如果这是一个人工子类,则为null。目前不提供动态创建非人工子类的机制。
  - var iVarDestroyer: UnsafeMutablePointer
    - 销毁实例变量的函数,用于在构造函数早期返回后进行清理。如果为null,则不会执行清理操作,并且所有的ivars都必须是简单的。

## struct TargetClassDescriptor

- struct TargetClassDescriptor
  - var flags: UInt32
    - 存储在任何上下文描述符的第一个公共标记
  - var parent: TargetRelativeDirectPointer
    - 复用的RelativeDirectPointer这个类型,其实并不是,但看下来原理一样;
    - 父级上下文,如果是顶级上下文则为null
  - var name: TargetRelativeDirectPointer
    - 获取类的名称
  - var accessFunctionPointer: TargetRelativeDirectPointer
    - 这里的函数类型是一个替身,需要调用getAccessFunction()拿到真正的函数指针(这里没有封装),会得到一个MetadataAccessFunction元数据访问函数的指针的包装器类,该函数提供operator()重载以使用正确的调用约定来调用它(可变长参数),意外发现命名重整会调用这边的方法(目前不太了解这块内容)。
  - var fieldDescriptor: TargetRelativeDirectPointer
    - 一个指向类型的字段描述符的指针(如果有的话)。类型字段的描述,可以从里面获取结构体的属性。
  - var superClassType: TargetRelativeDirectPointer

- The type of the superclass, expressed as a mangled type name that can refer to the generic arguments of the subclass type.
- Int32 Union (下面两个属性在源码中是union类型，所以取size大的类型作为属性（这里貌似一样），具体还得判断是否have a resilient superclass)
  - var ResilientMetadataBounds: RelativeDirectPointer
    - 有resilient superclass, 用ResilientMetadataBounds, 表示对保存元数据扩展的缓存的引用
  - var metadataNegativeSizeInWords: UInt32
    - 没有resilient superclass使用MetadataNegativeSizeInWords, 表示该类元数据对象的负大小(用字节表示)
- Int32 Union
  - var extraClassFlags: ExtraClassDescriptorFlags
    - 有resilient superclass, 用ExtraClassFlags, 表示一个Objective-C弹性类存根的存在
  - var metadataPositiveSizeInWords: UInt32
    - 没有resilient superclass使用MetadataPositiveSizeInWords, 表示该类元数据对象的正大小(用字节表示)
- var numImmediateMembers: UInt32
  - 此类添加到类元数据的其他成员的数目。默认情况下，这些数据对运行时是不透明的，而不是在其他成员中公开;它实际上只是NumImmediateMembers `sizeof(void)`字节的数据。
  - 这些字节是添加在地址点之前还是之后，取决于areImmediateMembersNegative()方法。
- var numFields: UInt32
  - 属性个数，不包含父类的
- var fieldOffsetVectorOffset: UInt32
  - 存储这个结构的字段偏移向量的偏移量（记录你属性起始位置的开始的一个相对于metadata的偏移量，具体看metadata的getFieldOffsets方法），如果为0，说明你没有属性
  - 如果这个类含有一个弹性的父类，那么从他的弹性父类的metaData开始偏移
- var Offset: UInt32
- var size: UInt32 //VTable数量
- var firstVtableData: VTableBuffer //VTable

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：  
2024-02-22 09:56:05

## Swift源码

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：  
2024-02-22 09:30:15

## IDA定义

```
struct ClassMetadata
{
 __int64 kind;
 void* superClass;
 __int64 cacheData[2];
 void* data;
 __int32 classFlags;
 __int32 instanceAddressPoint;
 __int32 instanceSize;
 __int16 instanceAlignmentMask;
 __int16 reserved;
 __int32 classSize;
 __int32 classAddressPoint;
 void* typeDescriptor;
 void* iVarDestroyer;
};
```

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:  
2024-02-22 10:22:49

## 举例

### \_\_DataStorage

具体详见：

ClassMetadata 内存布局 图

对应调试细节：

## ClassMetadata

```
(lldb) x /10xg 0x0000000207cb7d90
0x207cb7d90: 0x0000000207cb7d58 0x0000000207c47ed8
0x207cb7da0: 0x00000001c29c8490 0x0000805000000000
0x207cb7db0: 0x0000000281e95702 0x0000000000000002
0x207cb7dc0: 0x0000000700000041 0x00000010000000d0
0x207cb7dd0: 0x00000001b2009838 0x0000000000000000

(lldb) po 0x0000000207cb7d58
Foundation.__DataStorage
(lldb) po 0x0000000207c47ed8
_TtCs12_SwiftObject

(lldb) x /2xh 0x207cb7db8
0x207cb7db8: 0x0002 0x0000

(lldb) x /2xh 0x207cb7dc0
0x207cb7dc0: 0x0041 0x0000

(lldb) x /2xw 0x207cb7db8
0x207cb7db8: 0x00000002 0x00000000

(lldb) x /2xw 0x207cb7dc0
0x207cb7dc0: 0x00000041 0x00000007

(lldb) x /2xh 0x207cb7dc4
0x207cb7dc4: 0x0007 0x0000

(lldb) x /2xw 0x207cb7dc8
0x207cb7dc8: 0x000000d0 0x00000010
```

->

- \_\_DataStorage的Class的TypeMetadata
  - [+0x00] = var kind: Int
    - 0x0000000207cb7d58
      - Foundation.\_\_DataStorage
  - [+0x08] = var superClass: UnsafeMutablePointer
    - 0x0000000207c47ed8

- \_TtCs12\_SwiftObject
- [+0x10] = Int cacheData[2]
  - 0x00000001c29c8490
  - 0x0000805000000000
- [+0x20] = var data: Int
  - 0x0000000281e95702
- [+0x28] = var classFlags: UInt32
  - 0x00000002
- [+0x2C] = var instanceAddressPoint: UInt32
  - 0x00000000
- [+0x30] = var instanceSize: UInt32
  - 0x00000041
- [+0x34] = var instanceAlignmentMask: UInt16
  - 0x0007
- [+0x36] = var reserved: UInt16
  - 0x0000
- [+0x38] = var classSize: UInt32
  - 0x000000d0
- [+0x3C] = var classAddressPoint: UInt32
  - 0x00000010
- [+0x40] = var typeDescriptor: UnsafeMutablePointer
  - 0x00000001b2009838
- [+0x48] = var iVarDestroyer: UnsafeMutablePointer
  - 0x0000000000000000

以及：

## struct TargetClassDescriptor

```
(lldb) x 8xg 0x00000001b2009838
0x1b2009838: 0xfffffb3480000050 0xffff49e10fffffe8
0x1b2009848: 0x0000000000010464 0x0000001800000002
0x1b2009858: 0x000000060000000e 0x000000100000000a
0x1b2009868: 0x0000000100000008 0x00000001fff33690
(lldb) x/16xw 0x00000001b2009838
0x1b2009838: 0x80000050 0xfffffb34 0xfffffffffe8 0xffff49e10
0x1b2009848: 0x00010464 0x00000000 0x00000002 0x00000018
0x1b2009858: 0x0000000e 0x00000006 0x0000000a 0x00000010
0x1b2009868: 0x00000008 0x00000001 0xffff33690 0x00000001
```

->

- Foundation.\_\_DataStorage TypeDescriptor == struct TargetClassDescriptor
  - [+0x00] = var flags: UInt32
    - 0x80000050
  - [+0x04] = var parent: TargetRelativeDirectPointer
    - 0xfffffb34
  - [+0x08] = var name: TargetRelativeDirectPointer

- 0xffffffffe8
- [+0x0C] = var accessFunctionPointer: TargetRelativeDirectPointer
  - 0xffff49e10
- [+0x10] = var fieldDescriptor: TargetRelativeDirectPointer
  - 0x00010464
- [+0x14] = var superClassType: TargetRelativeDirectPointer
  - 0x00000000
- [+0x18] = Int32 Union
  - var ResilientMetadataBounds: RelativeDirectPointer
  - var metadataNegativeSizeInWords: UInt32
    - 估计是: 0x00000002
- [+0x1C] = Int32 Union
  - var extraClassFlags: ExtraClassDescriptorFlags
  - var metadataPositiveSizeInWords: UInt32
    - 暂不确定是哪个
    - 此处值: 0x00000018
- [+0x20] = var numImmediateMembers: UInt32
  - 0x0000000e
- [+0x24] = var numFields: UInt32
  - 0x00000006
- [+0x28] = var fieldOffsetVectorOffset: UInt32
  - 0x0000000a
- [+0x2C] = var Offset: UInt32
  - 0x00000010
- [+0x30] = var size: UInt32
  - 0x00000008
- [+0x34] = var firstVtableData: VTableBuffer
  - 0x00000001

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:  
2024-02-22 10:01:32

## MetadataKind = Metadata的type

Swift中Metadata的Type的定义

### 核心代码

```

const unsigned MetadataKindIsNonType = 0x400;
const unsigned MetadataKindIsNonHeap = 0x200;
const unsigned MetadataKindIsRuntimePrivate = 0x100;

LastEnumerated = 0x7FF,

NOMINALTYPEMETADATAKIND(Class, 0)
NOMINALTYPEMETADATAKIND(Struct, 0 | MetadataKindIsNonHeap)
NOMINALTYPEMETADATAKIND(Enum, 1 | MetadataKindIsNonHeap)
NOMINALTYPEMETADATAKIND(Optional, 2 | MetadataKindIsNonHeap)
METADATAKIND(ForeignClass, 3 | MetadataKindIsNonHeap)
METADATAKIND(Opaque, 0 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(Tuple, 1 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(Function, 2 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(Existential, 3 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(Metatype, 4 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(ObjCClassWrapper, 5 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)

METADATAKIND(ExistentialMetatype, 6 | MetadataKindIsRuntimePrivate | MetadataKindIsNonHeap)
METADATAKIND(HeapLocalVariable, 0 | MetadataKindIsNonType)
METADATAKIND(HeapGenericLocalVariable, 0 | MetadataKindIsNonType | MetadataKindIsRuntimePrivate)
METADATAKIND(ErrorObject, 1 | MetadataKindIsNonType | MetadataKindIsRuntimePrivate)

```



### 表格

| 名称           | 枚举值   | 说明                      |
|--------------|-------|-------------------------|
| Class        | 0x0   | 类                       |
| Struct       | 0x200 | 结构体                     |
| Enum         | 0x201 | 枚举                      |
| Optional     | 0x202 | 可选类型                    |
| ForeignClass | 0x203 | 外部类，比如CoreFoundation中的类 |
| Opaque       | 0x300 | 在元数据系统中不公开其值的类型         |
| Tuple        | 0x301 | 元祖类型                    |
| Function     | 0x302 | A monomorphic function  |
| Existential  | 0x303 | An existential type     |

|                          |       |                         |
|--------------------------|-------|-------------------------|
| Metatype                 | 0x304 | A metatype              |
| ObjCClassWrapper         | 0x305 | An ObjC class wrapper   |
| ExistentialMetatype      | 0x306 | An existential metatype |
| HeapLocalVariable        | 0x400 | 使用静态生成的元数据的堆分配的局部变量     |
| HeapGenericLocalVariable | 0x500 | 使用运行时实例化的元数据的堆分配的局部变量   |
| ErrorObject              | 0x501 | swift原生的错误类型            |
| LastEnumerated           | 0x7FF | 最大的非isa指针元数据类型值         |
| 下面是通用全局定义                |       |                         |
| MetadataKindIsNonType    | 0x400 |                         |
| MetadataKindIsNonHeap    | 0x200 |                         |
| MetadataKindIsNonHeap    | 0x200 |                         |
| LastEnumerated           | 0x7FF |                         |

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:

2024-02-22 10:12:10

# ValueBuffer

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：  
2024-02-22 09:30:05

## 常用类型

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：  
2024-02-22 09:31:52

# String字符串

## 空间占用=大小

- 空间占用: 0x10 字节 = 16 字节 = 2个 int64

## 分类=类型

### 概述

- Swift中String

- Small String

- Large String

- 三类

- Native

- 真正地址

```
realStrAddr = objectAddr + 0x20
 = objectAddr + 32
 = objectAddr + nativeBias
```

- Shared

- 真正地址

```
realStrAddr = objectAddr
```

- 说明

- 对于Bridge的字符串: objectAddr == NSString的地址

- 内存布局保存的数据, 是NSString中的数据

- Foreign

- 真正地址

```
realStrAddr = objectAddr
```

### 详解

- Swift中String

- Small String

- Large String

- 分3类

- native

- Native strings have tail-allocated storage, which begins at an offset of nativeBias from the storage object's address. String literals, which reside in the constant section, are encoded as their start address minus nativeBias, unifying code paths for both literals ("immortal native") and native strings. Native Strings are

always managed by the Swift runtime.

- shared

- Shared strings do not have tail-allocated storage, but can provide access upon query to contiguous UTF-8 code units. Lazily-bridged NSStrings capable of providing access to contiguous ASCII/UTF-8 set the ObjC bit. Accessing shared string's pointer should always be behind a resilience barrier, permitting future evolution.

- foreign

- Foreign strings cannot provide access to contiguous UTF-8. Currently, this only encompasses lazily-bridged NSStrings that cannot be treated as "shared". Such strings may provide access to contiguous UTF-16, or may be discontiguous in storage. Accessing foreign strings should remain behind a resilience barrier for future evolution. Other foreign forms are reserved for the future.

- 其他说明

- 对于Shared和foreign

- always created and accessed behind a resilience barrier, providing flexibility for the future.

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:

2024-02-22 09:31:53

# 内存布局

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：  
2024-02-22 09:27:09

## 图

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：  
2024-02-22 09:33:50

# 文字

## 概述

- Swift中Large String
  - Native
    - 真正字符串的地址=objectAddr+0x20
  - Shared/Foreign
    - 真正字符串的地址=objectAddr

## 详解

- Swift的String(64位)
  - 通用 (Small String和Large String都有)
    - discriminator
      - 关于名称和
      - 位置
        - == leading nibble == top nibble = 64bit的最顶部的4个bit: b63:b60 == [bit63 ~ bit60]
          - 注: nibble=半个字节 = 4bit
      - 名称
        - (此处有个专门的名字) discriminator = 辨别器: 用于区分字符串的具体类型
        - 其实叫做: String type 更加容易理解
      - 所以代码和注释中下面的名称是一个意思:
        - b63:b60 = discriminator = leading nibble == top nibble
    - 具体字段和含义
      - b63 = isImmortal
        - Should the Swift runtime skip ARC
          - Small strings are just values, always immortal
          - Large strings can sometimes be immortal, e.g. literals
      - b62 = (large) isBridged / (small) isASCII
        - For large strings, this means lazily-bridged NSString: perform ObjC ARC
        - Small strings repurpose this as a dedicated bit to remember ASCII-ness
      - b61 = isSmall
        - Dedicated bit to denote small strings
      - b60 = isForeign = isSlow
        - cannot provide access to contiguous UTF-8
      - 完整的映射表 = 不同字段的组合, 表示不同类型字符串

| Form             | b63 | b62   | b61 | b60 |
|------------------|-----|-------|-----|-----|
| Immortal, Small  | 1   | ASCII | 1   | 0   |
| Immortal, Large  | 1   | 0     | 0   | 0   |
| Native           | 0   | 0     | 0   | 0   |
| Shared           | x   | 0     | 0   | 0   |
| Shared, Bridged  | 0   | 1     | 0   | 0   |
| Foreign          | x   | 0     | 0   | 1   |
| Foreign, Bridged | 0   | 1     | 0   | 1   |

- Small String
  - [+0x00-0x0E] = 8+7个字节 = 15个字节 = 64+56位 = 120位 : realString
  - [+0xF] = 第16个字节=共8位: discriminator + count
    - byte15的[b4:b7] = discriminator
    - byte15的[b0:b3] = count
- Large String
  - [+0x00-0x07 ] = 8个字节 = 64位 : flag
    - b63 = ASCII = isASCII
    - b62 = NFC = isNFC
    - b61 = native = isNativelyStored
    - b60 = tail = isTailAllocated
    - b59 = UTF8 = isForeignUTF8
    - b58:48 = reserved
    - b47:0 = count
  - [+0x08-0x0F] = 8个字节 = 64位 : discriminator + objectAddr
    - b63:b60 = discriminator
      - 详见上述解释: b63 = isImmortal、b62 = (large) isBridged / (small) isASCII、b61 = isSmall、b60 = isForeign = isSlow
    - b60:b0 = objectAddr
      - realStrAddr = objectAddr + nativeBias = objectAddr + 32 = objectAddr + 0x20



## Swift源码

### StringObject.swift

- StringObject.swift
  - [swift/stdlib/public/core/StringObject.swift at main · apple/swift \(github.com\)](https://github.com/apple/swift/blob/main/stdlib/public/core/StringObject.swift)

```

extension _StringObject {
 @inlinable @inline(__always)
 internal init(_ small: _SmallString) {
 // Small strings are encoded as _StringObjects in reverse byte order
 // on big-endian platforms. This is to match the discriminator to the
 // spare bits (the most significant nibble) in a pointer.
 let word1 = small.rawBits.0.littleEndian
 let word2 = small.rawBits.1.littleEndian
#if _pointerBitWidth(_64)
 // On 64-bit, we copy the raw bits (to host byte order).
 self.init(rawValue: (word1, word2))
#elseif _pointerBitWidth(_32)
 // On 32-bit, we need to unpack the small string.
 let smallStringDiscriminatorAndCount UInt64 = 0xFF00_0000_0000_0000
 let leadingFour = Int(truncatingIfNeeded word1)
 let nextFour = UInt(truncatingIfNeeded word1 &>> 32)
 let smallDiscriminatorAndCount = word2 & smallStringDiscriminatorAndCount
 let trailingTwo = UInt16(truncatingIfNeeded word2)
 self.init(
 count: leadingFour,
 variant: .immortal(nextFour),
 discriminator: smallDiscriminatorAndCount,
 flags: trailingTwo)
#else
#error("Unknown platform")
#endif
 _internalInvariant(isSmall)
 }

 @inlinable
 internal static func getSmallCount(fromRaw x: UInt64) -> Int {
#if os(Android) && arch(arm64)
 return Int(truncatingIfNeeded: (x & 0x000F_0000_0000_0000) &>> 48)
#else
 return Int(truncatingIfNeeded: (x & 0x0F00_0000_0000_0000) &>> 56)
#endif
 }

 @inlinable @inline(__always)
 internal var smallCount: Int {
 _internalInvariant(isSmall)
 }
}

```

```

 return _StringObject.getSmallCount(fromRaw discriminatedObjectRawBits)
 }

 @inlinable
 internal static func getSmallIsASCII(fromRaw x: UInt64) -> Bool {
#if os(Android) && arch(arm64)
 return x & 0x0040_0000_0000_0000 != 0
#else
 return x & 0x4000_0000_0000_0000 != 0
#endif
}
@inlinable @inline(__always)
internal var smallIsASCII: Bool {
 _internalInvariant(isSmall)
 return _StringObject.getSmallIsASCII(fromRaw discriminatedObjectRawBits)
}

@inlinable @inline(__always)
internal init(empty: ()) {
 // Canonical empty pattern: small zero-length string
#if _pointerBitWidth(_64)
 self._countAndFlagsBits = 0
 self._object = Builtin.valueToBridgeObject(Nibbles.emptyString._value)
#elseif _pointerBitWidth(_32)
 self.init(
 count: 0,
 variant: .immortal(0),
 discriminator: Nibbles.emptyString,
 flags: 0)
#else
#error("Unknown platform")
#endif
 _internalInvariant(self.smallCount == 0)
 _invariantCheck()
}
}
}

```

## StringBridge.swift

swift/stdlib/public/core/StringBridge.swift

```

extension String {
 @_spi(Foundation)
 public init(_cocoaString: AnyObject) {
 self._guts = _bridgeCocoaString(_cocoaString)
 }
}

```

->

@usableFromInline

```

@_effects(releasenone) // @opaque
internal func _bridgeCocoaString(_ cocoaString _CocoaString) -> _StringGuts {
 switch _KnownCocoaString(cocoaString) {
 case .storage:
 return _unsafeUncheckedDowncast(
 cocoaString, to: __StringStorage.self).asString._guts
 case .shared:
 return _unsafeUncheckedDowncast(
 cocoaString, to: __SharedStringStorage.self).asString._guts
 #if _pointerBitWidth(_64)
 case .tagged:
 // Foundation should be taking care of tagged pointer strings before they
 // reach here, so the only ones reaching this point should be back deployed,
 // which will never have tagged pointer strings that aren't small, hence
 // the force unwrap here.
 return _StringGuts(_SmallString(taggedCocoa: cocoaString))
 #if arch(arm64)
 case .constantTagged:
 let taggedContents = getConstantTaggedCocoaContents(cocoaString)
 return _StringGuts(
 cocoa: taggedContents.untaggedCocoa,
 providesFastUTF8: false, //TODO: if contentsPtr is UTF8 compatible, use it
 isASCII: true,
 length: taggedContents.utf16Length
)
 #endif
 #endif
 case .cocoa:
 // "Copy" it into a value to be sure nobody will modify behind
 // our backs. In practice, when value is already immutable, this
 // just does a retain.
 //
 // TODO: Only in certain circumstances should we emit this call:
 // 1) If it's immutable, just retain it.
 // 2) If it's mutable with no associated information, then a copy must
 // happen; might as well eagerly bridge it in.
 // 3) If it's mutable with associated information, must make the call
 let immutableCopy
 = _stdlib_binary_CFStringCreateCopy(cocoaString)

 #if _pointerBitWidth(_64)
 if _isObjCTaggedPointer(immutableCopy) {
 // Copying a tagged pointer can produce a tagged pointer, but only if it's
 // small enough to definitely fit in a _SmallString
 return _StringGuts(
 _SmallString(taggedCocoa: immutableCopy).unsafelyUnwrapped
)
 }
 #endif

 let (fastUTF8, isASCII): (Bool, Bool)
 switch _getCocoaStringPointer(immutableCopy) {
 case .ascii(_): (fastUTF8, isASCII) = (true, true)
 case .utf8(_): (fastUTF8, isASCII) = (true, false)

```

```
default: (fastUTF8, isASCII) = (false, false)
}
let length = _stdlib_binary_CFStringGetLength(immutableCopy)

return _StringGuts(
 cocoa: immutableCopy,
 providesFastUTF8: fastUTF8,
 isASCII: isASCII,
 length: length)
}
}
```

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:  
2024-02-22 09:34:49

## IDA定义

加到IDA中的定义

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:  
2024-02-22 09:27:41

## 举例

### Small String

"control"

寄存器中：

```
(lldb) reg r x0 x1 sp
x0 = 0x006c6f72746e6f63
x1 = 0xe700000000000000
```

内存中：

```
(lldb) po 0x0000000281a4cea0
MainAppLibrary.OfflineAB.BucketInfo
(lldb) x 6xg 0x0000000281a4cea0
0x281a4cea0: 0x000000010415b460 0x0000000000000003
0x281a4ceb0: 0x006c6f72746e6f63 0xe700000000000000
0x281a4cec0: 0x0000000000002710 0x0000000281a4c930
(lldb) p c 0x006c6f72746e6f63
(long) control\0
```

->字符串本身 = realString :

```
0xe700000000000000 0x006c6f72746e6f63
```

->

```
(lldb) p c 0x006c6f72746e6f63
(unsigned long) control\0
```

->字符串是："control"

第15个字节=8位，分2部分：

- 最高4位=discriminator
  - 0xe
    - = 0b 1110
      - b63 = isImmortal -> 1
        - isImmortal=True
      - b62 = (large) isBridged / (small) isASCII -> 1
        - Small String: ASCII=True
      - b61 = isSmall -> 1
        - 是Small string
      - b60 = isForeign = isSlow -> 0
        - isForeign=False

- 最低4位=count
  - 0x7
    - 字符串长度是: 7
    - = 7个字符
    - 对应着: control字符串的长度=7

## Large String

### Large String - Native

"ios\_prod\_latam\_tos\_reg\_universe"

```
(lldb) po 0x00000002800f5e00
MainAppLibrary.OfflineAB.UniverseInfo

(lldb) x/6gx 0x00000002800f5e00
0x2800f5e00: 0x0000000105d3c398 0x0000000200000003
0x2800f5e10: 0xd000000000000001f 0x8000000105110930
0x2800f5e20: 0x6469725f72657375 0xe800000000000000
```

根据定义:

- MainAppLibrary.OfflineAB.UniverseInfo
  - [+0x10~0x18] = name
    - 类型: Swift的Large String (真正字符串地址是: name值+0x20)

此处值:

- [+0x10~0x18] = name
  - 0x2800f5e10: 0xd000000000000001f 0x8000000105110930

-》 真正字符串地址是:

- 0x8000000105110930 + 0x20 = 0x8000000105110950

```
(lldb) x/s 0x8000000105110950
0x105110950: "ios_prod_latam_tos_reg_universe"
```

### 额外说明

(1) 如果不加0x20, 则看到的字符串是别的 (错位后的) 值:

```
(lldb) x/s 0x8000000105110930
0x105110930: "os_reg_experiment"
```

(2) 去掉最开始的0x8, 也是可以用x/s看到字符串的:

```
(lldb) x/s 0x0000000105110930
0x105110930: "os_reg_experiment"
(lldb) x/s 0x0000000105110950
```

```
0x105110950: "ios_prod_latam_tos_reg_universe"
```

类似的：去掉0x8前缀，可以用po查看出字符串的值：

```
(lldb) po (char*)0x00000000105110950
"ios_prod_latam_tos_reg_universe"
```

(3) 不论是否加0x20，直接po查看，则都是（异常的，不是我们要的）时间类型的值：

```
(lldb) po 0x80000000105110930
2001 01 01 00 00 00 - 0000
(lldb) po 0x80000000105110950
2001 01 01 00 00 00 - 0000

(lldb) po (char*)0x80000000105110950
2001 01 01 00 00 00 - 0000
```

后记：

另外某次去po，却连异常的时间类型的值都看不到，而是：就是数字：

```
(lldb) reg r x0 x1
 x0 = 0x0000000000000007c
 x1 = 0xe100000000000000
(lldb) reg r x20 sp
 x20 = 0x0000000016d658c20
 sp = 0x0000000016d658c20
(lldb) x 8gx 0x0000000016d658c20
0x16d658c20: 0xd0000000000000021 0x800000001051946f0
0x16d658c30: 0x00000000000000002 0x00000002833c1140
0x16d658c40: 0x00000000105da1628 0x00000000105dbbcd0
0x16d658c50: 0x000000002833c1140 0x000000002828d0780
(lldb) po 0x800000001051946f0
9223372041235285744
```

而换x/s字符串查看，是可以看出：

（虽然是错误的，但是是）字符串的值的

```
(lldb) x s 0x800000001051946f0
0x1051946f0: "dummy_aa_offline_user_rid_ios"
```

当然，真正地址+0x20的字符串：

```
(lldb) p x 0x800000001051946f0 + 0x20
(unsigned long) 0x80000000105194710
```

->但是po也还是看不出：

```
(lldb) po 0x80000000105194710
```

```
9223372041235285776
```

只能用字符串查看：

```
(lldb) x s 0x80000000105194710
0x105194710: "dummy_aa_offline_rid_universe_ios"
```

## Large String - Shared

### "2.23.25.85"

此处：

```
0xc000000000000000a 0x400000028143c6c0
```

其中：

- Large String
  - 0xc000000000000000a
    - 0xC = 12 = 0b 1100
      - b63 = ASCII = isASCII
        - True
      - b62 = NFC = isNFC
        - True
      - b61 = native = isNativelyStored
        - False
      - b60 = tail = isTailAllocated
        - False
      - b59 = UTF8 = isForeignUTF8
        - False
    - 0xa = 10 : 字符串长度是10
  - 0x400000028143c6c0
    - discriminator = 0x4 = 0b 0100
      - b63 = isImmortal
        - False
      - b62 = (large) isBridged / (small) isASCII
        - True
      - b61 = isSmall
        - False
      - b60 = isForeign = isSlow
        - False
    - objectAddr = 0x28143c6c0

->

- Large String
  - length = 10

- flag
  - isASCII = True
  - isNFC = True
  - isNativelyStored = False
  - isTailAllocated = False
  - isForeignUTF8 = False
- discriminator
  - isImmortal = False
  - isBridged = True
  - isSmall = False
  - isForeign == isSlow = False
- objectAddr = 0x28143c6c0

->

- Swift中的字符串
  - 是bridged桥接的
  - 字符串地址是: 0x28143c6c0
  - 其他细节
    - 是ASCII的
    - 是NFC (Normal Form C) 的
    - 不是尾部分配的TailAllocated

-> 此处对应着: 从 objc 的 NSString : "2.23.25.85"

```
(lldb) reg r x0
x0 = 0x000000028143c6c0
(lldb) po $x0
2.23.25.85
(lldb) po [$x0 class]
__NSCFString
```

调用

- libswiftFoundation.dylib
  - static
 

```
Swift.String._unconditionallyBridgeFromObjectiveC(Swift.Optional<__C.NSString>) ->
Swift.String
```

而Bridge桥接过来的

->

此处: 想要查看出字符串的值:

- (方式1) 加上NSString强制类型转换去打印字符串

```
(lldb) po (NSString*)0x000000028143c6c0
2.23.25.85
```

- (方式2) 自己查看ObjC的NSString的内存值，手动打印出字符串

此处 (NSString类型的字符串的) 内存值是：

```
(lldb) x &g 0x00000028143c6c0
0x28143c6c0: 0x000021a1efdfa941 0x000000030000078c
0x28143c6d0: 0x35322e33322e320a 0x0000000000035382e
0x28143c6e0: 0x00004fcde1ddc6e0 0x0000000000000001
0x28143c6f0: 0x0000000000000000 0x0000000000000000
```

其中核心数据是：

- 0x28143c6d0: 0x35322e33322e320a 0x0000000000035382e

->可以调试查看到具体字符串的值和长度：

```
(lldb) p c 0x35322e33322e320a
(long) \n2.23.25
(lldb) p c 0x0000000000035382e
(int) .85\0

(lldb) x &b 0x28143c6d0
0x28143c6d0: 0x0a 0x32 0x2e 0x32 0x33 0x2e 0x32 0x35
(lldb) x &b 0x28143c6d8
0x28143c6d8: 0x2e 0x38 0x35 0x00 0x00 0x00 0x00 0x00
(lldb) x s 0x28143c6d0
0x28143c6d0: "\n2.23.25.\0"
(lldb) x s 0x28143c6d8
0x28143c6d8: ".85"

(lldb) p d 0xa
(int) 10
(lldb) x s 0x28143c6d1
0x28143c6d1: "2.23.25.\0"
```

即：

- 字符串：
  - 长度： 10
  - 值： 2.23.25.\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：  
2024-02-22 09:31:12

# Array数组

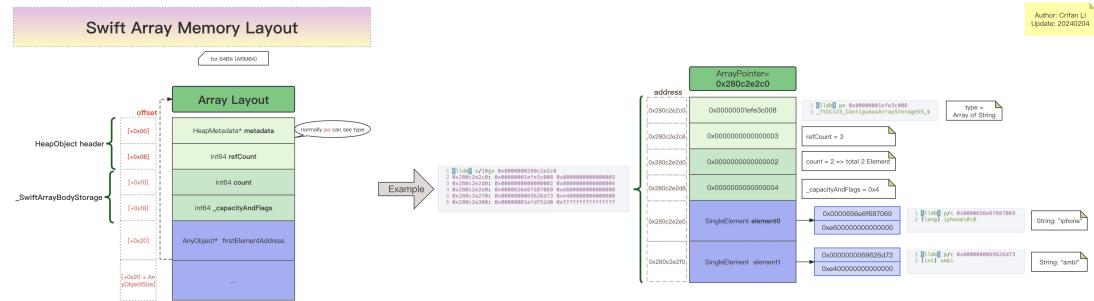
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:33:13

# 内存布局

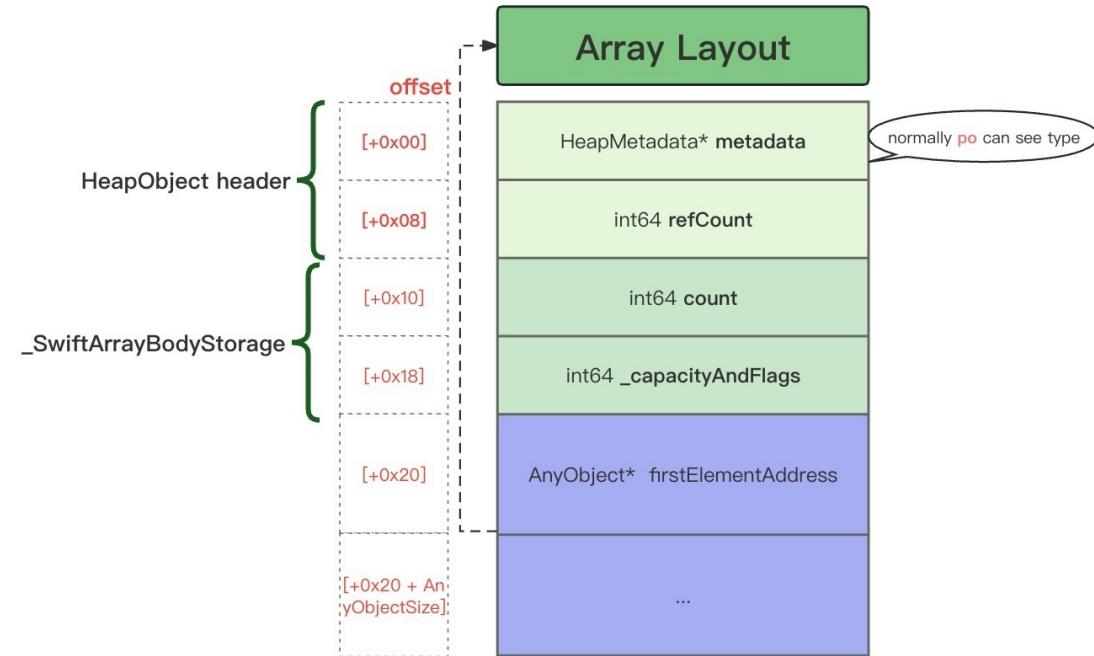
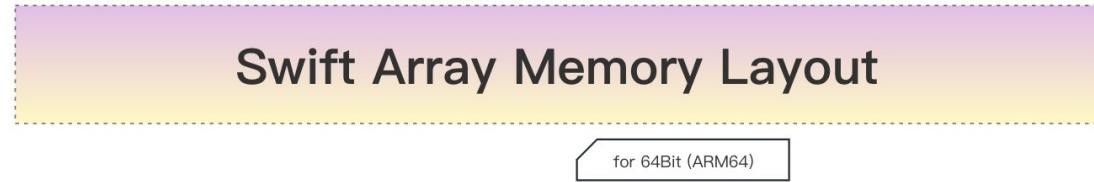
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:26:12

# Swift的Array的内存布局图

- Swift的Array的内存布局图 = Swift Array Memory Layout
  - 在线预览
    - [Swift的Array内存布局结构图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)
  - 离线查看



- 核心内容



## 文字

- Array的内存布局=字段=属性
  - [+0x00] = HeapMetadata\* metadata
  - [+0x08] = int64 refCount
  - [+0x10] = int64 count
  - [+0x08] = int64 \_capacityAndFlags
  - [+0x20] = AnyObject\* firstElementAddress

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：  
2024-02-22 10:24:24

## Swift源码

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：  
2024-02-22 09:31:12

## IDA定义

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：  
2024-02-22 09:34:49

## 举例

### String的Array

```
(lldb) x 10gx 0x0000000280c2e2c0
0x280c2e2c0: 0x00000001efe3c008 0x00000000000000000003
0x280c2e2d0: 0x00000000000000000002 0x00000000000000000004
0x280c2e2e0: 0x0000656e6f687069 0xe6000000000000000000
0x280c2e2f0: 0x00000000069626d73 0xe4000000000000000000
0x280c2e300: 0x00000001efd52d0 0x7fffffff7fffffff
(lldb) po 0x00000001efe3c008
_TtGCs23_ContiguousArrayStorageSS_$
(lldb) p c 0x0000656e6f687069
(long) iphone\0\0
(lldb) p c 0x00000000069626d73
(int) smbi
```

->

- Array的内存布局=字段
  - HeapMetadata\* metadata
    - 0x00000001efe3c008
      - `_TtGCs23_ContiguousArrayStorageSS_$`
      - String的Array
  - int64 refCount
    - 0x0000000000000003
  - int64 count
    - 0x0000000000000002
  - int64 \_capacityAndFlags
    - 0x0000000000000004
  - 第一个 = [0x280c2e2e0]
    - 0x0000656e6f687069 0xe600000000000000
      - "iphone"
  - 第二个 = [0x280c2e2f0]
    - 0x00000000069626d73 0xe400000000000000
      - "smbi"

# Set集合

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：  
2024-02-22 09:30:32

# 内存布局

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：  
2024-02-22 09:33:40

## 图

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：  
2024-02-22 09:34:58

# 文字

## 概述

## 详解

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:  
2024-02-22 09:28:42

## Swift源码

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：  
2024-02-22 09:33:27

## IDA定义

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：  
2024-02-22 09:29:47

## 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：  
2024-02-22 09:27:16

# Dictionary字典

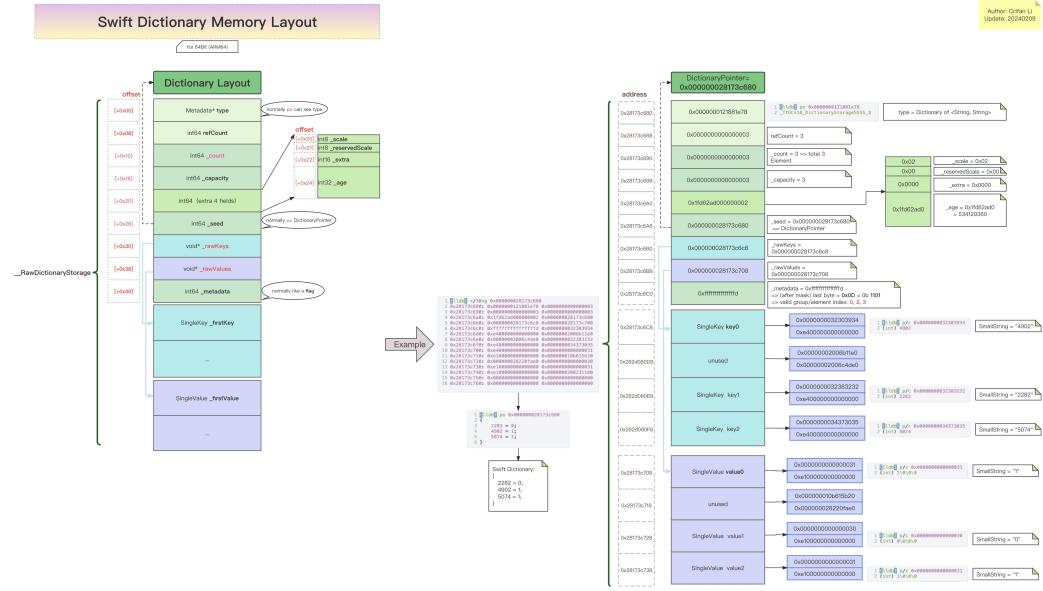
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:35:12

## Swift的Dictionary内存布局

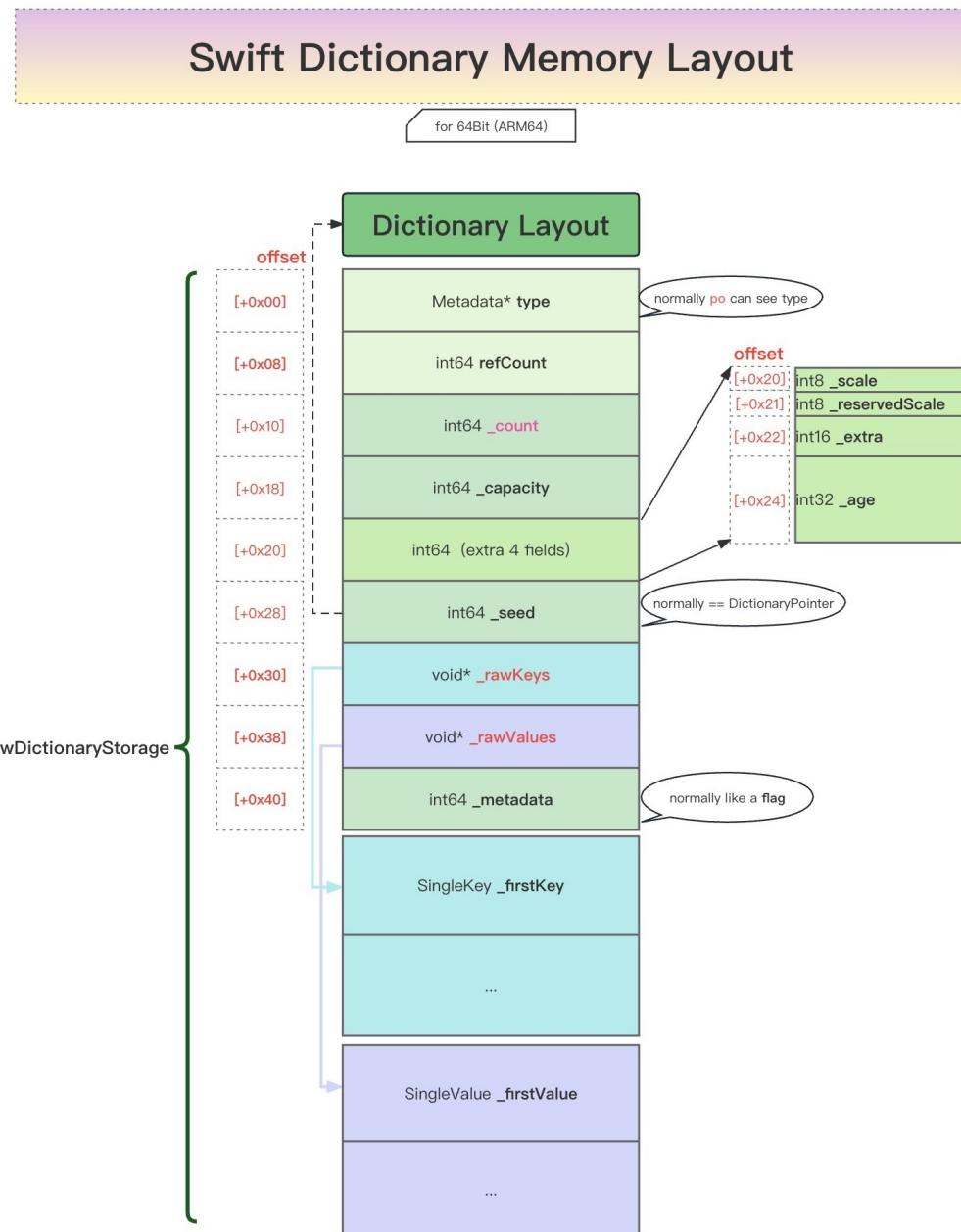
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:34:24

# Swift的Dictionary内存布局结构图

- Swift的Dictionary内存布局结构图
  - 在线浏览
    - [Swift的Dictionary内存布局结构图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)
  - 本地查看
    - [完整图](#)



- 核心内容



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:  
2024-02-22 09:27:46

## Swift的Dictionary内存布局 文字

- Swift的Dictionary内存布局 = 字段 = 属性
  - [+0x00] = Metadata\* type
  - [+0x08] = Int refCount
  - \_\_RawDictionaryStorage
    - [+0x10] = var \_count: Int
    - [+0x18] = var \_capacity: Int
    - [+0x20] = Int
      - [+0x20~0x20] = var \_scale: Int8
      - [+0x21~0x21] = var \_reservedScale: Int8
      - [+0x22~0x23] = var \_extra: Int16
      - [+0x24~0x27] = var \_age: Int32
    - [+0x28] = var \_seed: Int
    - [+0x30] = var \_rawKeys: UnsafeMutableRawPointer
      - 指向 Key = 键 的数组列表
    - [+0x38] = var \_rawValues: UnsafeMutableRawPointer
      - 指向 value = 值 的数组列表
    - [+0x38] = int \_metadata
      - 指定了哪几个index元素是有效数据

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:  
2024-02-22 09:28:14

## Swift源码

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：  
2024-02-22 09:32:46

## IDA定义

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：  
2024-02-22 09:32:16

## 举例

### 举例1：简单dict

Swift的Dict值：

```
{
 2282 = 0;
 4902 = 1;
 5074 = 1;
}
```

对应的例子，已经放到了内存布局图中了，详见：

[Dictionary字典的内存布局图](#)

此处只额外贴出：

## 相关调试内容

```
(lldb) po 0x0000000028173c680
{
 2282 = 0;
 4902 = 1;
 5074 = 1;
}
```

->

```
(lldb) x 8xg 0x0000000028173c680
0x28173c680: 0x0000000121881e78 0x00000000000000000003
0x28173c690: 0x000000000000000003 0x00000000000000000003
0x28173c6a0: 0x1fd62ad0000000002 0x000000028173c680
0x28173c6b0: 0x000000028173c6c8 0x000000028173c708
(lldb) x /20xg 0x0000000028173c680
0x28173c680: 0x0000000121881e78 0x00000000000000000003
0x28173c690: 0x000000000000000003 0x00000000000000000003
0x28173c6a0: 0x1fd62ad0000000002 0x000000028173c680
0x28173c6b0: 0x0000000028173c6c8 0x0000000028173c708
0x28173c6c0: 0xfffffffffffffffffffffd 0x0000000032303934
0x28173c6d0: 0xe400000000000000 0x000000002006b11e0
0x28173c6e0: 0x000000002006c4de0 0x0000000032383232
0x28173c6f0: 0xe400000000000000 0x0000000034373035
0x28173c700: 0xe400000000000000 0x000000000000000031
0x28173c710: 0xe100000000000000 0x0000000010b615b20
```

可以继续了：

- 0xd = 0b 1101

- 有效index
  - 0
  - 2
  - 3

-&gt;

```
(lldb) x/40xg 0x000000028173c680
0x28173c680: 0x0000000121881e78 0x0000000000000003
0x28173c690: 0x0000000000000003 0x0000000000000003
0x28173c6a0: 0x1fd62ad00000002 0x000000028173c680
0x28173c6b0: 0x000000028173c6c8 0x000000028173c708
0x28173c6c0: 0xfffffffffffd 0x0000000032303934
0x28173c6d0: 0xe400000000000000 0x00000002006b11e0
0x28173c6e0: 0x00000002006c4de0 0x0000000032383232
0x28173c6f0: 0xe400000000000000 0x0000000034373035
0x28173c700: 0xe400000000000000 0x0000000000000031
0x28173c710: 0xe100000000000000 0x0000000010b615b20
0x28173c720: 0x000000028220fae0 0x0000000000000030
0x28173c730: 0xe100000000000000 0x0000000000000031
0x28173c740: 0xe100000000000000 0x0000000280231180
0x28173c750: 0x0000000000000000 0x0000000000000000
0x28173c760: 0x0000000000000000 0x0000000000000000
0x28173c770: 0x0000000000000000 0x0000000000000000
0x28173c780: 0x0000000000000000 0x0000000000000000
0x28173c790: 0x0000000000000000 0x0000000000000000
0x28173c7a0: 0x0000000000000000 0x0000000000000000
0x28173c7b0: 0x0000000000000000 0x0000000000000000

(lldb)
```

```
(lldb) x/30xg 0x000000028173c680
0x28173c680: 0x0000000121881e78 0x0000000000000003
0x28173c690: 0x0000000000000003 0x0000000000000003
0x28173c6a0: 0x1fd62ad00000002 0x000000028173c680
0x28173c6b0: 0x000000028173c6c8 0x000000028173c708
0x28173c6c0: 0xfffffffffffd 0x0000000032303934
0x28173c6d0: 0xe400000000000000 0x00000002006b11e0
0x28173c6e0: 0x00000002006c4de0 0x0000000032383232
0x28173c6f0: 0xe400000000000000 0x0000000034373035
0x28173c700: 0xe400000000000000 0x0000000000000031
0x28173c710: 0xe100000000000000 0x0000000010b615b20
0x28173c720: 0x000000028220fae0 0x0000000000000030
0x28173c730: 0xe100000000000000 0x0000000000000031
0x28173c740: 0xe100000000000000 0x0000000280231180
0x28173c750: 0x0000000000000000 0x0000000000000000
0x28173c760: 0x0000000000000000 0x0000000000000000
```

-&gt;

```
(lldb) po 0x0000000121881e78
_TtGCs18_DictionaryStorageSSSS_$

(lldb) p c 0x0000000032303934
(int) 4902
```

```
(lldb) p c 0x0000000032383232
(int) 2282
(lldb) p c 0x0000000034373035
(int) 5074
(lldb) p c 0x000000000000000031
(int) 1\0\0\0
(lldb) p c 0x000000000000000030
(int) 0\0\0\0
(lldb) x 2xw 0x28173c6a0
0x28173c6a0: 0x00000002 0x1fd62ad0
(lldb) x /4xh 0x28173c6a0
0x28173c6a0: 0x0002 0x0000 0x2ad0 0x1fd6
(lldb) x /8xb 0x28173c6a0
0x28173c6a0: 0x02 0x00 0x00 0x00 0xd0 0x2a 0xd6 0x1f
(lldb) p d 0x1fd62ad0
(int) 534129360
```

## 举例2：复杂dict - key是String, value是AnyPrimitive

调试到复杂dict：

```
(lldb) reg r x0 x1 x2 x8
 x0 = 0x000000011100b200
 x1 = 0x00000001031145b0 WhatsApp`$s10LeafFilterVN
 x2 = 0x0000000103114658 WhatsApp`LeafFilter_related_1030B4658
 x8 = 0x00000001006409a8 WhatsApp`sub_1005E09A8
(lldb) po 0x000000011100b200
4580225536
(lldb) x 6xg 0x000000011100b200
0x11100b200: 0x000000010fe175c8 0x00000000000000000003
0x11100b210: 0x00000000000000000007 0x0000000000000000000c
0x11100b220: 0xf3473a6200000004 0x000000011100b200
(lldb) po 0x000000010fe175c8
_TtGCs18_DictionaryStorageSSOV014MainAppLibrary90fflineAB8UserInfoP10$102e672c012AnyPrimitive_$
```

->

此处是个Dictionary, value元素是

- AnyPrimitive
  - MainAppLibrary.OfflineAB.UserInfo 的 AnyPrimitive

查看内存值：

```
(lldb) x 80xg 0x000000011100b200
0x11100b200: 0x000000010fe175c8 0x00000000000000000003
0x11100b210: 0x00000000000000000007 0x0000000000000000000c
0x11100b220: 0xf3473a6200000004 0x000000011100b200
0x11100b230: 0x000000011100b248 0x000000011100b348
0x11100b240: 0xfffffff9299 0x6d726f6674616c70
0x11100b250: 0xe800000000000000 0x00000001e84fab78
0x11100b260: 0x00000001e84fab78 0x00000001e84fab78
```

```

0x11100b270: 0x00000001e84fab78 0x695f656369766564
0x11100b280: 0xe9000000000000064 0x69737265765f736f
0x11100b290: 0xea00000000006e6f 0x00000001e84fab78
0x11100b2a0: 0x00000001e84fab78 0x00000001e84fab78
0x11100b2b0: 0x00000001e84fab78 0x6c6975625f707061
0x11100b2c0: 0xe9000000000000064 0x00000001e84fab78
0x11100b2d0: 0x00000001e84fab78 0x6e5f656369766564
0x11100b2e0: 0xeb0000000656d61 0x00000001e84fab78
0x11100b2f0: 0x00000001e84fab78 0x00000001e84fab78
0x11100b300: 0x00000001e84fab78 0x5f657361656c6572
0x11100b310: 0xef6c656e6e616863 0x00000001e84fab78
0x11100b320: 0x00000001e84fab78 0x00000001e84fab78
0x11100b330: 0x00000001e84fab78 0x737265765f707061
0x11100b340: 0xeb00000006e6f69 0x0000656e6f687069
0x11100b350: 0xe6000000000000000 0x000000010fe17468
0x11100b360: 0x000000010fe16950 0x000000010fe169f8
0x11100b370: 0x00000001e84fab01 0x00000001e84fab78
0x11100b380: 0x00000001e84fab78 0x00000001e84fab78
0x11100b390: 0x00000001e84fab78 0x00000001e84fab78
0x11100b3a0: 0x00000001e84fab78 0x00000001e84fab78
0x11100b3b0: 0x00000001e84fab78 0x00000001e84fab78
0x11100b3c0: 0x00000001e84fab78 0x00000001e84fab78
0x11100b3d0: 0x00000001e84fab78 0xc0000000000000024
0x11100b3e0: 0x40000002820700c0 0x00000002820700c0
0x11100b3f0: 0x000000010fe16950 0x000000010fe169f8
0x11100b400: 0x00000001e84fab01 0x000000014164cccd
0x11100b410: 0xc00000000000000a 0x40000002835413a0
0x11100b420: 0x000000010fe17798 0x000000010fe17840
0x11100b430: 0x00000001e84fab00 0x00000001e84fab78
0x11100b440: 0x00000001e84fab78 0x00000001e84fab78
0x11100b450: 0x00000001e84fab78 0x00000001e84fab78
0x11100b460: 0x00000001e84fab78 0x00000001e84fab78
0x11100b470: 0x00000001e84fab78 0x00000001e84fab78

```

-&gt;

```

(lldb) p c 0x6d726f6674616c70
(long) platform

(lldb) p c 0x695f656369766564
(long) device_i
(lldb) p c 0xe9000000000000064
(unsigned long) d\0\0\0\0\0\xe9

(lldb) p c 0x69737265765f736f
(long) os_versi
(lldb) p c 0xea00000000006e6f
(unsigned long) on\0\0\0\0\0\xea

(lldb) p c 0x6c6975625f707061
(long) app_buil
(lldb) p c 0x64
(int) d\0\0\0

(lldb) p c 0x6e5f656369766564

```

```
(long) device_n
(lldb) p c 0x00000000656d61
(int) ame\0

(lldb) p c 0x5f657361656c6572
(long) release_
(lldb) p c 0xef6c656e6e616863
(unsigned long) channel\xef

(lldb) p c 0x737265765f707061
(long) app_vers
(lldb) p c 0xeb000000006e6f69
(unsigned long) ion\0\0\0\0\xeb
```

keys:

- platform
- device\_id
- os\_version
- app\_build
- device\_name
- release\_channel
- app\_version
- iphone

和:

```
(lldb) p c 0x0000656e6f687069
(long) iphone\0\0

(lldb) x s "0x40000002820700c0 + 0x20"
0x2820700e0: "5E8-8164-1AEA05E45CD9"
(lldb) po 0x00000002820700c0
2DE85147 8D62 45E8 8164 1AEA05E45CD9
...
...
```

values:

- iphone
- 2DE85147-8D62-45E8-8164-1AEA05E45CD9
  - 注: Swift的Shared=Bridged的String
- ...

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:  
2024-02-22 09:27:14

## Struct结构体

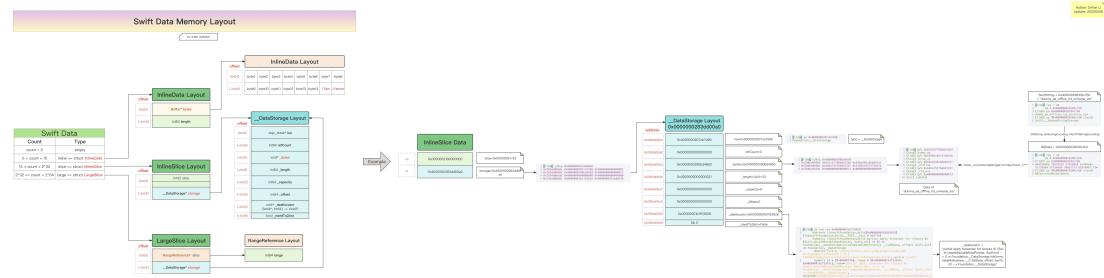
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:34:38

## Data数据的内存布局

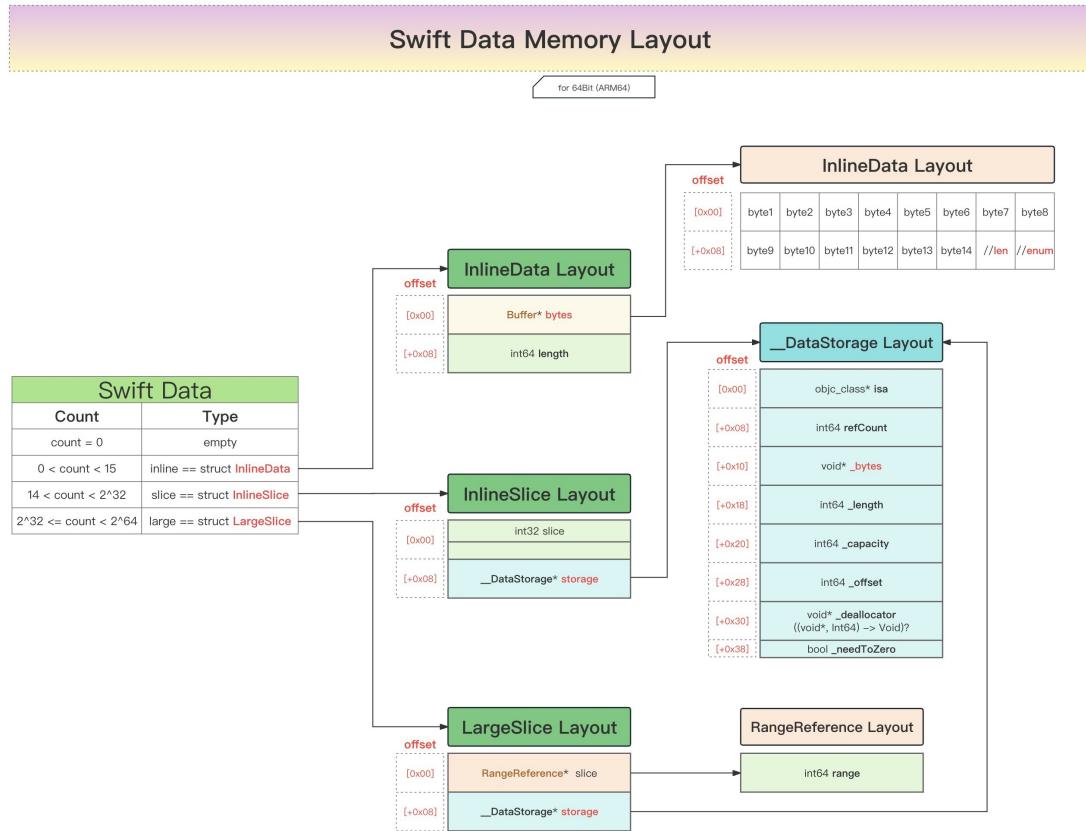
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：  
2024-02-22 09:42:22

# Swift的Data数据的内存布局结构图

- Swift的Data数据的内存布局结构图 = Swift Data Memory Layout
  - 在线预览
    - [Swift的Data内存布局结构图| ProcessOn免费在线作图,在线流程图,在线思维导图](#)
  - 离线查看



- 核心内容



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：  
2024-02-22 09:41:58

# 文字

## 概述

- Swift的Data（对于64位，暂忽略32位）的内存布局
  - 根据数据字节个数多少分类
    - count=0
      - empty = 空数据
    - 0 < count < 15 == 0 < count <= 14
      - inline == structInlineData
        - var bytes: Buffer
          - @usableFromInline typealias Buffer = (UInt8, UInt8, UInt8, UInt8,
 UInt8, UInt8, UInt8, UInt8, UInt8, UInt8, UInt8, UInt8,
 UInt8) //len //enum
        - var length: UInt8
    - 14 < count < 2^32
      - slice == structInlineSlice
        - var slice: Range<Int32>
        - var storage: \_\_DataStorage
    - 2^32 <= count < 2^64
      - large == structLargeSlice
        - var slice: RangeReference
          - var range: Range<Int64>
        - var storage: \_\_DataStorage

### \_\_DataStorage

```
class __DataStorage {
 var isa: objc_class* // NULL for pure Swift class
 var refCount: UInt64
 var _bytes: UnsafeMutableRawPointer?
 var _length: UInt64
 var _capacity: UInt64
 var _offset: UInt64
 var _deallocator: ((UnsafeMutableRawPointer, Int64) -> Void)?
 var _needToZero: Bool
}
```

==

- class \_\_DataStorage
  - [+0x00] = objc\_class\* isa
  - [+0x08] = int64 refCount
  - [+0x10] = void\* \_bytes
  - [+0x18] = int64 \_length

- [+0x20] = int64 \_capacity
- [+0x28] = int64 \_offset
- [+0x30] = function\_pointer\* \_deallocator
  - 函数定义: ((UnsafeMutableRawPointer, Int64) -> Void)?
- [+0x38] = Bool \_needToZero

## 详解

- Swift的Data
  - 分4类
    - 空数据: empty
    - inline == structInlineData
      - 字段
        - var bytes: Buffer
        - var length: UInt8
      - 说明
        - bytes的Buffer的字节=个数
        - 64位架构: 不超过14, 即 <=14个字节
          - @usableFromInline typealias Buffer = (UInt8, UInt8, UInt8) //len //enum
        - 32位架构: 不超过6, 即 <=6个字节
          - @usableFromInline typealias Buffer = (UInt8, UInt8, UInt8, UInt8, UInt8, UInt8) //len //enum
    - slice == struct InlineSlice
      - 字段
        - var slice: Range
        - var storage: \_\_DataStorage
      - 说明
        - InlineData的 (64bit的) 14个 < InlineSlice的字节个数 < 2^64的最大值? (storage pointer + range == a signle word)
    - large == struct LargeSlice
      - 字段
        - var slice: RangeReference
        - var range: Range
        - var storage: \_\_DataStorage
      - 说明
        - a single word个数=2^64? < LargeSlice的字节个数 < 双字节大小 (two-word size) =2^128?

## Swift源码

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:  
2024-02-22 09:35:57

## IDA定义

- struct Swift\_DataStorage

```
struct Swift_DataStorage
{
 void isa;
 __int64 refCount;
 void *_bytes;
 __int64 _length;
 __int64 _capacity;
 __int64 _offset;
 void *_deallocator;
 bool _needToZero;
};
```

- struct SwiftData\_InlineSlice

```
struct SwiftData_InlineSlice
{
 __int32 slice;
 Swift_DataStorage storage;
};
```

## 举例

### \_\_DataStorage

详见：

[Data数据 内存布局 图](#)

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：  
2024-02-22 09:43:31

# 内存布局

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：  
2024-02-22 09:25:57

## 图

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：  
2024-02-22 09:35:07

# 文字

## 概述

## 详解

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:  
2024-02-22 09:33:04

## Swift源码

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：  
2024-02-22 09:34:28

## IDA定义

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：  
2024-02-22 09:28:05

## 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：  
2024-02-22 09:26:37

# Bool布尔

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：  
2024-02-22 09:29:42

# Enum枚举

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：  
2024-02-22 09:29:07

# Tuple元祖

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：  
2024-02-22 09:31:47

## Int整型

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：  
2024-02-22 09:32:26

## 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：  
2024-02-22 09:33:24

## 参考资料

- 【已解决】iOS逆向Swift：Dictionary字典的内存布局结构
- 【已解决】iOS逆向Swift：找Swift的Dictionary字典的测试数据
- 【整理】iOS逆向：去画Swift的Dictionary字典的内存布局结构图
- 【未解决】iOS逆向WhatsApp：genWAABOfflineAssignSha256\_10039E294
- 【已解决】iOS逆向：Swift中String字符串的内部结构和逻辑
- 【已解决】iOS逆向Swift：研究\_unconditionallyBridgeFromObjectiveC后的SwiftString的值的逻辑和含义
- 【未解决】iOS逆向Swift：String.\_unconditionallyBridgeFromObjectiveC
- 【已解决】iOS逆向Swift：VWT=ValueWitnessTable=值见证表
- 【已解决】iOS逆向Swift：IDA优化插入ValueWitnessTable结构体定义
- 【已解决】iOS逆向Swift：IDA中自定义结构体中加上bit位的定义
- 【已解决】iOS逆向Swift：BuiltIn.NativeObject的VWT
- 【已解决】iOS逆向Swift：Data数据的内存布局结构
- 【已解决】iOS逆向Swift：Data的InlineSlice内存布局举例
- 【已解决】iOS逆向Swift：画Swift的Data数据的内存布局结构图
- 【未解决】iOS逆向Swift：IDA中添加Swift的Data相关定义
- 【已解决】iOS逆向Swift：画ClassMetadata的内存布局结构图
- 【整理】iOS逆向：去画Swift的ValueMetadata和VWT的内存布局结构图
- 【已解决】iOS逆向Swift：ClassMetadata的定义和内存布局
- 【未解决】iOS逆向Swift：\_\_DataStorage的ClassMetadata内存布局值举例
- 【已解决】iOS逆向Swift：Metadata的type即元数据的类型定义
- 【已解决】iOS逆向Swift：ValueMetadata的定义和内存布局结构
- 【已解决】iOS逆向Swift：IDA中加上定义：ValueMetadata
- 【已解决】iOS逆向Swift：StructMetadata的字段定义和内存布局结构
- 【已解决】iOS逆向Swift：Swift中有几种Metadata
- 【已解决】iOS逆向Swift：TypeMetadata=Type Metadata
- 【已解决】iOS逆向Swift：IDA中添加ClassMetadata的定义
- 【已解决】iOS逆向Swift：Array数组的内存布局
- 【整理】iOS逆向：去画Swift的Array数组的内存布局结构图
- 【已解决】iOS逆向Swift：StructMetadata的字段定义和内存布局结构
- 【已解决】iOS逆向Swift：StructDescriptor
- 【已解决】iOS逆向Swift：FieldDescriptor
- 【已解决】iOS逆向Swift：画StructMetadata的内存布局图
- 
- 初探Swift底层Metadata - 掘金
- [swift-evolution/proposals/0247-contiguous-strings.md at main · apple/swift-evolution \(github.com\)](https://github.com/apple/swift-evolution/blob/main/proposals/0247-contiguous-strings.md)
- [swift/docs/CppInteroperability/CppInteroperabilityManifesto.md at main · apple/swift](https://apple swift/docs/CppInteroperability/CppInteroperabilityManifesto.md)
-

