C# Format

CLI Header size: 0x48

| Offset | Size | Field | Description |
| --- | --- | --- | --- |
| 0 | 4 | Cb | Size of the header in bytes |
| 4 | 2 | MajorRuntimeVersion | The minimum version of the runtime required to run this program, currently 2. |
| 6 | 2 | MinorRuntimeVersion | The minor portion of the version, currently 0. |
| 8 | 8 | MetaData | RVA and size of the physical metadata (§[24](file:///D:\software\Partition%20II%20Metadata.doc#_Metadata_Physical_Layout)). |
| 16 | 4 | Flags | Flags describing this runtime image. (§[25.3.3.1](file:///D:\software\Partition%20II%20Metadata.doc#_Runtime_Flags)). |
| 20 | 4 | EntryPointToken | Token for the *MethodDef* or File of the entry point for the image |
| 24 | 8 | Resources | RVA and size of implementation-specific resources. |
| 32 | 8 | StrongNameSignature | RVA of the hash data for this PE file used by the CLI loader for binding and versioning |
| 40 | 8 | CodeManagerTable | Always 0 (§[24.1](file:///D:\software\Partition%20II%20Metadata.doc#_Fixed_Fields)). |
| 48 | 8 | VTableFixups | RVA of an array of locations in the file that contain an array of function pointers (e.g., vtable slots), see below. |
| 56 | 8 | ExportAddressTableJumps | Always 0 (§[24.1](file:///D:\software\Partition%20II%20Metadata.doc#_Fixed_Fields)). |
| 64 | 8 | ManagedNativeHeader | Always 0 (§[24.1](file:///D:\software\Partition%20II%20Metadata.doc#_Fixed_Fields)). |

Runtime Flags

| Flag | Value | Description |
| --- | --- | --- |
| COMIMAGE\_FLAGS\_ILONLY | 0x00000001 | Always 1 (§[24.1](file:///D:\software\Partition%20II%20Metadata.doc#_Fixed_Fields)). |
| COMIMAGE\_FLAGS\_32BITREQUIRED | 0x00000002 | Image can only be loaded into a 32-bit process, for instance if there are 32-bit vtablefixups, or casts from native integers to int32. CLI implementations that have 64-bit native integers shall refuse loading binaries with this flag set. |
| COMIMAGE\_FLAGS\_STRONGNAMESIGNED | 0x00000008 | Image has a strong name signature. |
| COMIMAGE\_FLAGS\_TRACKDEBUGDATA | 0x00010000 | Always 0 (§[24.1](file:///D:\software\Partition%20II%20Metadata.doc#_Fixed_Fields)). |

例子：

TEST.exe

Flags : 0x00 02 00 03

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0F | 0E | 0D | 0C | 0B | 0A | 09 | 08 | 07 | 06 | 05 | 04 | 03 | 02 | 01 | 00 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

格式

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0F** | **0E** | **0D** | **0C** | **0B** | **0A** | **09** | **08** | **07** | **06** | **05** | **04** | **03** | **02** | **01** | **00** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1F | 1E | 1D | 1C | 1B | 1A | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2F | 2E | 2D | 2C | 2B | 2A | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3F | 3E | 3D | 3C | 3B | 3A | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

例子

1 1110,0000,1001,

0011,1111,1011,0111 ,

1011,1111,0101,0111

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0F** | **0E** | **0D** | **0C** | **0B** | **0A** | **09** | **08** | **07** | **06** | **05** | **04** | **03** | **02** | **01** | **00** |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1F | 1E | 1D | 1C | 1B | 1A | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 2F | 2E | 2D | 2C | 2B | 2A | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 |
|  |  |  | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 3F | 3E | 3D | 3C | 3B | 3A | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

43 - 0x2B

#~ stream

offset : 0x2F30D8

0x00 Module

0x01 TypeRef

0x02 TypeDef

0x03 FieldPtr

0x04 Field

0x05 MethodPtr

0x06 MethodDef

0x07 ParamPtr

0x08 Param

0x09 InterfaceImpl

0x0A MemberRef

0x0B Constant

0x0C CustomAttribute

0x0D FieldMarshal

0x0E DeclSecurity

0x0F ClassLayout

0x10 FieldLayout

0x11 StandAloneSig

0x12 EventMap

0x13 EventPtr

0x14 Event

0x15 PropertyMap

0x16 PropertyPtr

0x17 Property

0x18 MethodSemantics

0x19 MethodImpl

0x1A ModuleRef

0x1B TypeSpec

0x1C ImplMap

0x1D FieldRVA

0x1E ENCLog

0x1F ENCMap

0x20 Aseembly

0x21 AssemblyProcessor

0x22 AssemblyOS

0x23 AssemblyRef

0x24 AssemblyRefProcessor

0x25 AssemblyRefOS

0x26 File

0x27 ExportedType

0x28 ManifestResource

0x29 NestedClass

0x2A GenericParam

0x2B MethodSpec

0x2C GenericParamConstraint

指令集合

MONO\_CUSTOM\_PREFIX 0xf0

OPDEF(CEE\_NOP, "nop", Pop0, Push0, InlineNone, X, 1, 0xFF, 0x00, NEXT)

#define OPDEF(a,b,c,d,e,f,g,h,I,j) MONO\_ ## a,

typedef enum{

MONO\_CEE\_NOP,

MONO\_CEE\_LAST

}MonoOpcodeEnum;

typedef struct{

unsigned char argument;

unsigned char flow\_type;

unsigned short opval;

}MonoOpcode;

#define OPDEF(a,b,c,d,e,f,g,h,i,j) \

{ Mono ## e, MONO\_FLOW\_ ## j, MONO\_ ## a },

Mono\_InlineNone

MONO\_FLOW\_NEXT

MONO\_CEE\_NOP

ILASM

C:\Windows\Microsoft.NET\Framework\v4.0.30319

C:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.6.1 Tools

ildasm

C# 基础知识

什么是Field ？

什么是Event ？

## Mono.Cecil 加载流程分析

ModuleDefinition 构造函数里创建MetadataReader

0x4cab98 – 0x2000 = 0x4c8b98

0x4c8c04 = 0x4c8b98 + 0x6c #~

MetaDataRoot

Section.RVA 0x2000

MetaData.RVA 0x4cab98 元数据相对Section的offset

0x6c 相对元数据的offset

TableHeap 相对 section的offset

0x4c8c04 + 0x200 = 0x4c8e04

0x53000001 0 0x0001 Module(1)

0x0000053E 1 0x0541 TypeRef(1345)

0x00002143 2 0x2145 TypeDef(8517)

0x0000E419 0xE40A Field(58378)

0x0000F8B1 0xF8B7 Method(63671)

0x0000A1C7 0xA1D5 Param(41429)

0x0000062C 0x0626 InterfaceImpl(1574)

0x0000325B 0x31B1 MemberRef(12721)

0x00004D1C 0x4D1F Constant(19743)

0x000021F3 0x21E8 CustomAttribute(8680)

0x000000E1 0x00E1 FieldMarshal(225)

0x00000022 0x0022 ClassLayout(34)

0x00000009 0x0009 FieldLayout(9)

0x00002588 0x258C StandAloneSig(9612)

0x00000030 0x0030 EventMap(48)

0x0000008E 0x008E Event(142)

0x00000711 0x0710 PropertyMap(1808)

0x00001A90 0x1A8D Property(6797)

0x00002640 0x263D MethodSemantics(9789)

0x0000037C 0x0372 MethodImpl(882)

0x00000009 0x0009 ModuleRef(9)

0x0000075B 0x075C TypeSpec(1884)

0x0000010B 0x010B ImplMap(267)

0x00000038 0x0039 FieldRVA(57)

0x00000001 0x0001 Assembly(1)

0x000E AssemblyRef(14)

0x0626 NestedClass(1574)

0x012C GenericParam(300)

0x0B56 MethodSpec(2902)

0x00C3

The “#~” streams contain the actual physical representations of the logical metadata tables (§[22](#_Metadata_Logical_Format:_2)\_21\_Metedata\_Logical\_Format\_Tables). A “#~” stream has the following top-level structure:

| Offset | Size | Field | Description |
| --- | --- | --- | --- |
| 0 | 4 | Reserved | Reserved, always 0 (§[24.1](#_Fixed_Fields)). |
| 4 | 1 | MajorVersion | Major version of table schemata; shall be 2 (§[24.1](#_Fixed_Fields)). |
| 5 | 1 | MinorVersion | Minor version of table schemata; shall be 0 (§[24.1](#_Fixed_Fields)). |
| 6 | 1 | HeapSizes | Bit vector for heap sizes. |
| 7 | 1 | Reserved | Reserved, always 1 (§[24.1](#_Fixed_Fields)). |
| 8 | 8 | Valid | Bit vector of present tables, let *n* be the number of bits that are 1. |
| 16 | 8 | Sorted | Bit vector of sorted tables. |
| 24 | 4\**n* | Rows | Array of *n* 4-byte unsigned integers indicating the number of rows for each present table. |
| 24+4\*n |  | Tables | The sequence of physical tables. |

The HeapSizes field is a bitvector that encodes the width of indexes into the various heaps. If bit 0 is set, indexes into the “#String” heap are 4 bytes wide; if bit 1 is set, indexes into the “#GUID” heap are 4 bytes wide; if bit 2 is set, indexes into the “#Blob” heap are 4 bytes wide. Conversely, if the HeapSize bit for a particular heap is not set, indexes into that heap are 2 bytes wide.

| **Heap size flag** | **Description** |
| --- | --- |
| 0x01 | Size of “#String” stream >= 216. |
| 0x02 | Size of “#GUID” stream >= 216. |
| 0x04 | Size of “#Blob” stream >= 216. |