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 ？