1. 文件标志

文件标志占用8个字节，格式如下：

|  |  |  |
| --- | --- | --- |
| 标识符 | 类型 | 说明 |
| signature | char[5] | 标志，必须为”YCOFF” |
| version | byte | 文件格式版本，必须为1 |
| macflag | byte | Bit0：表示机器大小端  0: Little Endian  1: Big Endian  Bit1~Bit2：表示机器字长  0: 32-bit  1: 64-bit  2: 128-bit |
| filetype | byte | 1: 可重定位文件(\*.o)  2: 可执行文件(\*.exe)  3: 动态链接库(\*.dll) |

1. COFF文件头

|  |  |  |
| --- | --- | --- |
| 标识符 | 类型 | 说明 |
| magic | ushort | 表示机器类型  0x14c: x86  0x8664: x86-64 |
| numofsec | ushort | Section节的个数  如果数值为0xffff，则采用可选头中的数值代替 |
| timedate32 | Uint | 文件创建的时间戳  如果数值为0xffffffff，则采用可选头中的数值代替 |
| symptr | uint | COFF符号表偏移 |
| numofsym | uint | COFF符号的个数 |
| opthdrsize | U16 | 可选头的大小 |
| Flags | U16 | COFF文件属性标志 |

| **Flag** | **Value** | **Description** |
| --- | --- | --- |
| IMAGE\_FILE\_RELOCS\_STRIPPED | 0x0001 | Image only, Windows CE, and Windows NT® and later. This indicates that the file does not contain base relocations and must therefore be loaded at its preferred base address. If the base address is not available, the loader reports an error. The default behavior of the linker is to strip base relocations from executable (EXE) files. |
| IMAGE\_FILE\_EXECUTABLE\_IMAGE | 0x0002 | Image only. This indicates that the image file is valid and can be run. If this flag is not set, it indicates a linker error. |
| IMAGE\_FILE\_LINE\_NUMS\_STRIPPED | 0x0004 | COFF line numbers have been removed. This flag is deprecated and should be zero. |
| IMAGE\_FILE\_LOCAL\_SYMS\_STRIPPED | 0x0008 | COFF symbol table entries for local symbols have been removed. This flag is deprecated and should be zero. |
| IMAGE\_FILE\_AGGRESSIVE\_WS\_TRIM | 0x0010 | Obsolete. Aggressively trim working set. This flag is deprecated for Windows 2000 and later and must be zero. |
| IMAGE\_FILE\_LARGE\_ADDRESS\_ AWARE | 0x0020 | Application can handle > 2‑GB addresses. |
|  | 0x0040 | This flag is reserved for future use. |
| IMAGE\_FILE\_BYTES\_REVERSED\_LO | 0x0080 | Little endian: the least significant bit (LSB) precedes the most significant bit (MSB) in memory. This flag is deprecated and should be zero. |
| IMAGE\_FILE\_32BIT\_MACHINE | 0x0100 | Machine is based on a 32-bit-word architecture. |
| IMAGE\_FILE\_DEBUG\_STRIPPED | 0x0200 | Debugging information is removed from the image file. |
| IMAGE\_FILE\_REMOVABLE\_RUN\_ FROM\_SWAP | 0x0400 | If the image is on removable media, fully load it and copy it to the swap file. |
| IMAGE\_FILE\_NET\_RUN\_FROM\_SWAP | 0x0800 | If the image is on network media, fully load it and copy it to the swap file. |
| IMAGE\_FILE\_SYSTEM | 0x1000 | The image file is a system file, not a user program. |
| IMAGE\_FILE\_DLL | 0x2000 | The image file is a dynamic-link library (DLL). Such files are considered executable files for almost all purposes, although they cannot be directly run. |
| IMAGE\_FILE\_UP\_SYSTEM\_ONLY | 0x4000 | The file should be run only on a uniprocessor machine. |
| IMAGE\_FILE\_BYTES\_REVERSED\_HI | 0x8000 | Big endian: the MSB precedes the LSB in memory. This flag is deprecated and should be zero. |

1. **Auxiliary Header**