1. 文件标志

文件标志占用8个字节，格式如下：start:0

|  |  |  |  |
| --- | --- | --- | --- |
| 标识符 | 类型 | offset | 说明 |
| f\_sign | char[5] | 0 | 标志，必须为”YCOFF” |
| f\_ver | byte | 5 | 文件格式版本，必须为1 |
| f\_cpuflag | byte | 6 | Bit0：表示机器字长  0: 32-bit  1: 64-bit  Bit1：表示机器大小端  0: Little Endian  1: Big Endian |
| f\_ftype | byte | 7 | 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 （28/32字节）start:8

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 标识符 | COFF32 | | COFF64 | | 说明 |
| 大小 | offs | 大小 | offs |
| f\_magic | 2 | 0/8 | 2 | 0/8 | 表示机器类型  0x14c: x86  0x8664: x86-64 |
| f\_flags | 2 | 2/10 | 2 | 2/10 | COFF文件属性标志 |
| f\_nscns | 4 | 4/12 | 4 | 4/12 | Section节的个数 |
| f\_timdat | 8 | 8/16 | 8 | 8/16 | 文件创建的时间戳 |
| f\_symptr | 4 | 16/24 | 8 | 16/24 | COFF符号表偏移 |
| f\_nsyms | 4 | 20/28 | 4 | 24/32 | COFF符号的个数 |
| f\_auxhsz | 4 | 24/32 | 4 | 28/36 | 辅助文件头的大小 |

其中，flags每一位的含义是：

|  |  |
| --- | --- |
| 0x0001 | 重定位信息已经被移除 |
| 0x0002 | 文件可以执行， exe和dll必须设置 |
| 0x0004 | 保留 |
| 0x0008 | 保留 |
| 0x0010 | 保留 |
| 0x0020 | 能处理2GB以上内存地址，64位机器需要置1 |
| 0x0040 | 保留 |
| 0x0080 | 保留 |
| 0x0100 | 保留 |
| 0x0200 | 保留 |
| 0x0400 | 保留 |
| 0x0800 | 保留 |
| 0x1000 | 保留 |
| 0x2000 | 该文件是动态链接库DLL或者是动态对象（.so） |
| 0x4000 | 保留 |
| 0x8000 | 保留 |

三、辅助文件头 (可执行镜像) start:36/40

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 标识符 | COFF32 | | COFF64 | | 说明 |
| 大小 | offs | 大小 | offs |
| a\_amagic | 2 | 0 | 2 | 0 | 辅助文件头标志，为0 |
| a\_lnkver1 | 1 | 2 | 1 | 2 | 连接器主版本 |
| a\_lnkver2 | 1 | 3 | 1 | 3 | 连接器次版本 |
| a\_checksum | 4 | 28 | 4 | 4 | 文件校验和 |
| a\_tsize | 4 | 4 | 8 | 8 | Text总大小，代码段总大小 |
| a\_dsize | 4 | 8 | 8 | 16 | Data总大小，数据段总大小 |
| a\_bsize | 4 | 12 | 8 | 24 | bss总大小，未初始化数据段总大小 |
| a\_entry | 4 | 16 | 8 | 32 | 程序入口点（RVA），没有入口点，则必须为0 |
| a\_text\_start | 4 | 20 | 8 | 40 | Text的起始地址（RVA） |
| a\_data\_start | 4 | 24 | 8 | 48 | Data的起始地址（RVA） |
| o\_stacksz | 4 |  | 8 | 56 | Specifies the maximum stack size (in bytes) allowed for this executable. If the value is 0, the system default maximum stack size is used. |
| o\_heap | 4 |  | 8 | 64 | Specifies the in heap size (in bytes) allowed for this executable. If the value is 0, the system default maximum stack size is used. |
| a\_lddtptr | 4 |  | 4 | 68 | LDDT表在文件中的偏移 |
| a\_lddtsz | 4 |  | 4 | 72 | LDDT表的项数 |
| a\_aitptr | 4 |  | 4 | 76 | Additional Information Table表在文件中的偏移 |
| a\_aitsz | 4 |  | 4 | 80 | Additional Information Table表的项数 |
| a\_uuid0 | 4 | 32 | 4 | 84 | 文件的UUID |
| a\_uuid1 | 4 |  | 4 | 88 | 文件的UUID |
| a\_uuid2 | 4 |  | 4 | 92 | 文件的UUID |
| a\_uuid3 | 4 |  | 4 | 96 | 文件的UUID |
| a\_secagn | 4 |  | 4 | 100 | Section的内存对齐 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | 4 |  |  |  |  |
|  | 4 |  |  |  |  |
|  | 4 |  |  |  |  |
|  | 4 |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Auxiliary Header**