

# EXE File Format

By unknown

offset	length	description	comments
0	word	exe file signature	usually 4d5a
2	word	length of last used sector in file	modulo 512
4	word	size of file, incl. header	in 512-pages
6	word	number of relocation table items	
8	word	size of header	in 16-byte paragraphs
a	word	min. paragraphs needed above program	in 16-byte paragraphs
c	word	max. paragraphs needed above program	in 16-byte paragraphs
e	word	displacement of stack segment in module	rel. to start of prog.
10	word	contents of SP reg. at entry	
12	word	checksum	2's complement
14	word	contents of IP reg. at entry	
16	word	displacement of code module	rel. to start of prog.
18	word	offset to first relocation item in file	rel. to start of prog.
1a	word	overlay number	0 for resident prog.
1c	varies	variable RESERVED place	
varies	varies	relocation table	
varies	varies	variable RESERVED place	
varies	varies	program and data space	
varies	varies	stack segment	

The relocation table is a set of far pointers (eg: 1234:5678h) and it appears you just add the relocation factor to the value at that address. The relocation factor is the start segment of where the program is loaded.

Example:

```
-----  
code segment  
start:  
    mov  ax,seg _myseg  
code ends
```

```
_myseg segment  
_myseg ends  
end start
```

Start	Stop	Length	Name	Class
00000H	00002H	00003H	CODE	
00010H	00010H	00000H	_MYSEG	

Note that \_MYSEG is exactly one segment above CODE.

Generated output is B8 01 00; which is "mov ax,0001"

The fixup table for this file has a single entry, 0000:0001. Thus if the start of the program begins at segment 3562 then the "mov ax,0001" gets converted to "mov ax,3563".