

- ③ 可选文件头中:
- AddressOfEntryPoint PE 装载器准备运行的PE文件的第一条指令的RVA
 - ImageBase PE 文件在内存中的优先装载地址
 - SectionAlignment 内存中节对齐粒度
 - FileAlignment 文件中节对齐粒度

机器类型x86 节数目 生产该文件的时间 COFF符号表的偏移

test.exe程序-PE文件格式分析

姓名: 曹海琪 学号: 2018302180132

		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
PE文件固定开头 MZ的ASCII码																		
IMAGE_DOS_HEADER	00000000h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	: MZ?..... ..
	00000010h:	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	: ;?.....@.....
	00000020h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	:
	00000030h:	00	00	00	00	00	00	00	00	00	00	00	00	B0	00	00	00	: 转向PE文件头开始?置
	00000040h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	: ..?.???L?Th
MS-DOS Stub Program	00000050h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	: ;is program canno
	00000060h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	: ;t be run in DOS
	00000070h:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	: ;mode...\$......
	00000080h:	5D	65	FD	C8	19	04	93	9B	19	04	93	9B	19	04	93	9B	: ;le..搽..搽..搽
	00000090h:	97	1B	80	9B	11	04	93	9B	E5	24	81	9B	18	04	93	9B	: ;?€?.搽?仁..搽
signature PE标志“PE\0\0” 识别是否为有效PE文件	000000a0h:	52	69	63	68	19	04	93	9B	00	00	00	00	00	00	00	00	: ;Rich..搽.....
	000000b0h:	50	45	00	00	4C	01	03	00	9B	4D	8F	42	00	00	00	00	: ;PE..L...汆度....
	000000c0h:	00	00	00	00	E0	00	0F	01	0B	01	05	0C	00	02	00	00	: ;符其数?..可选文件头大小 文件信息标志
	000000d0h:	00	04	00	00	00	00	00	00	00	10	10	00	00	00	10	00	: ;AddressOfEntryPoint
	000000e0h:	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00	: ;ImageBase@.SectionAlignment FileAlignment
IMAGE_NT_HEADERS ① signature ② FileHeader 映像文件头 (0x14) ③ OptionalHeader 可选文件头	000000f0h:	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	: ;.....
	00000100h:	00	40	00	00	00	04	00	00	00	00	00	00	02	00	00	00	: ;.@.....
	00000110h:	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	: ;.....
	00000120h:	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	: ;NumberofDirectoriesEXPORT Table
	00000130h:	14	20	00	00	3C	00	00	00	00	00	00	00	00	00	00	00	: ;IMPORT TableSource Table
Directory 前四个字节: RVA 后四个字节: size	00000140h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000150h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000160h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000170h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000180h:	00	00	00	00	00	00	00	00	00	20	00	00	14	00	00	00	: ;EXPORT Address Table
IMAGE_SECTION_- HEADER	00000190h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	000001a0h:	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	: ;.....text... 代码节
	000001b0h:	46	00	00	00	00	10	00	00	00	02	00	00	00	04	00	00	: ;F..... 代码节
	000001c0h:	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	: ;.....
	000001d0h:	2E	72	64	61	74	61	00	00	A6	00	00	00	00	20	00	00	: ;.rdata..?.... 引出函数节
	000001e0h:	00	02	00	00	00	06	00	00	00	00	00	00	00	00	00	00	: ;.....@...@ data... 已初始化的数据节
	000001f0h:	00	00	00	00	40	00	00	40	2E	64	61	74	61	00	00	00	: ;.....@...@ data... 已初始化的数据节
	00000200h:	8E	00	00	00	00	30	00	00	00	02	00	00	00	08	00	00	: ;?...0.....@..?
	00000210h:	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0	: ;.....@..?
	00000220h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000230h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000240h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000250h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000260h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000270h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000280h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
	00000290h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	: ;.....
		节表的名称	虚拟大小	虚拟偏移量	Raw大小	Raw偏移												

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000002a0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000002b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000002c0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000002d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000002e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000002f0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000300h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000310h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000320h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000330h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000340h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000350h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000360h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000370h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000380h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000390h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003a0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003c0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000003f0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000400h:	68	40	10	00	00	68	00	30	40	00	68	09	30	40	00	6A	; h@...h.0@.h.0@.j
00000410h:	00	E8	2A	00	00	00	68	40	10	00	68	00	30	40	00	00	; ?...h@...h.0@.
00000420h:	68	31	30	40	00	6A	00	E8	14	00	00	00	6A	00	E8	01	; h10@.j.?...j.?
00000430h:	00	00	00	CC	FF	25	00	20	40	00	FF	25	0C	20	40	00	; ...?%.@.%.@.
00000440h:	FF	25	08	20	40	00	00	00	00	00	00	00	00	00	00	00	; %.@.....
00000450h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000460h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000470h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000480h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000490h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004a0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004c0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
000004f0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000500h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000510h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000520h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000530h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000540h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000550h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000560h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000570h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;
00000580h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;

test.exe 程序-PE 文件格式分析

姓名: _____ 学号: _____

0 1 2 3 4 5 6 7 8 9 A B C D E F

MZ 文件头

- MZ 标识符
- PE 文件头入口地址

PE 文件头

PE 标识符

映像文件头

- 运行平台(I386)
- 文件中节的数目
- 文件的生成时间
- 可选文件头的大小

可选文件头

- PE 文件第一条运行指令的RVA
- 代码节RVA
- 引入函数节RVA
- PE 文件优先装载地址 (Image Base)
- 内存中节的粒度
- 文件中节的粒度

数据目录表

(16表项, 每项8字节。表项结构为4字节的表RVA与4字节的表大小)

- 引出函数节表项
- 引入函数节表项
- 资源节表项
- IAT表项

00000000h:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	; MZ?..... ..
00000010h:	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	; ?......@.....
00000020h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000030h:	00 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00	;?..
00000040h:	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	; ..?.???L?Th
00000050h:	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	; is program canno
00000060h:	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	; t be run in DOS
00000070h:	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	; mode....\$......
00000080h:	5D 65 FD C8 19 04 93 9B 19 04 93 9B 19 04 93 9B	;]e ..椿..椿..椿
00000090h:	97 1B 80 9B 11 04 93 9B E5 24 81 9B 18 04 93 9B	; ?e?.椿?仁..椿
000000a0h:	52 69 63 68 19 04 93 9B 00 00 00 00 00 00 00 00	; Rich..椿.....
000000b0h:	50 45 00 00 4C 01 03 00 9B 4D 8F 42 00 00 00 00	; PE..L...汭厦...
000000c0h:	00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00	;?.....
000000d0h:	00 04 00 00 00 00 00 00 00 10 00 00 00 10 00 00	;
000000e0h:	00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00	;@.....
000000f0h:	04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00	;
00000100h:	00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00	; ..@.....
00000110h:	00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00	;
00000120h:	00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00	;
00000130h:	14 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00	; ...<.....
00000140h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000150h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000160h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000170h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000180h:	00 00 00 00 00 00 00 00 00 20 00 00 14 00 00 00	;
00000190h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000001a0h:	00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00	;text...
000001b0h:	46 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00	; F.....`
000001c0h:	00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60	;
000001d0h:	2E 72 64 61 74 61 00 00 A6 00 00 00 00 20 00 00	; ..rdata..?...
000001e0h:	00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00	;
000001f0h:	00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00	;@..@.data...
00000200h:	8E 00 00 00 00 30 00 00 02 00 00 00 00 08 00 00	; ?...0.....
00000210h:	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0	;@..?
00000220h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000230h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000240h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000250h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000260h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000270h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000280h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000290h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;

DOS 桩

0 1 2 3 4 5 6 7 8 9 A B C D E F

000002a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000002b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000002c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000002d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000002e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000002f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000300h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000310h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000320h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000330h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000340h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000350h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000360h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000370h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000380h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000390h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000003f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000400h:	68 40 10 00 00 68 00 30 40 00 68 09 30 40 00 6A	; h@...h.0@.h.0@.j
00000410h:	00 E8 2A 00 00 00 68 40 10 00 00 68 00 30 40 00	; .?...h@...h.0@.
00000420h:	68 31 30 40 00 6A 00 E8 14 00 00 6A 00 E8 01	; h10@.j.?...j.?
00000430h:	00 00 00 CC FF 25 00 20 40 00 FF 25 0C 20 40 00	; ...?%. @. %. @.
00000440h:	FF 25 08 20 40 00 00 00 00 00 00 00 00 00 00 00	; %..@.....
00000450h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000460h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000470h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000480h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000490h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000004f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000500h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000510h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000520h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000530h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000540h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000550h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000560h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	; %..@.....
00000570h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00000580h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;

节表

(本例包含代码节、引入函数节、数据节3个表项, 每表项20字节)

- 节名称(.text)
- 节的RVA
- 节的长度
- 节在文件中的位置
- 节属性

代码节

test.exe 程序-PE 文件格式分析

姓名: _____ 学号: _____

0 1 2 3 4 5 6 7 8 9 A B C D E F

MZ 文件头

- MZ 标识符
- PE 文件头入口地址

PE 文件头

PE 标识符

映像文件头

- 运行平台(I386)
- 文件中节的数目
- 文件的生成时间
- 可选文件头的大小

可选文件头

- PE 文件第一条运行指令的RVA
- 代码节RVA
- 引入函数节RVA
- PE 文件优先装载地址 (Image Base)
- 内存中节的粒度
- 文件中节的粒度

数据目录表

(16表项, 每项8字节。表项结构为4字节的表RVA与4字节的表大小)

- 引出函数节表项
- 引入函数节表项
- 资源节表项
- IAT表项

00000000h:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?..... ..
00000010h:	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....
00000020h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030h:	00 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00?..
00000040h:	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..?.???L?Th
00000050h:	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00000060h:	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00000070h:	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....\$......
00000080h:	5D 65 FD C8 19 04 93 9B 19 04 93 9B 19 04 93 9B]e ..椿..椿..椿
00000090h:	97 1B 80 9B 11 04 93 9B E5 24 81 9B 18 04 93 9B	?e?.椿?仁..椿
000000a0h:	52 69 63 68 19 04 93 9B 00 00 00 00 00 00 00 00	Rich..椿.....
000000b0h:	50 45 00 00 4C 01 03 00 9B 4D 8F 42 00 00 00 00	PE..L...汭厦...
000000c0h:	00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00?.....
000000d0h:	00 04 00 00 00 00 00 00 00 10 00 00 00 10 00 00
000000e0h:	00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00@.....
000000f0h:	04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
00000100h:	00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00@.....
00000110h:	00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00
00000120h:	00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00
00000130h:	14 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00	...<.....
00000140h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000150h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000170h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180h:	00 00 00 00 00 00 00 00 00 20 00 00 14 00 00 00
00000190h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001a0h:	00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00text...
000001b0h:	46 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00	F.....`
000001c0h:	00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60
000001d0h:	2E 72 64 61 74 61 00 00 A6 00 00 00 00 20 00 00	..rdata..?..
000001e0h:	00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00
000001f0h:	00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00@..@.data...
00000200h:	8E 00 00 00 00 30 00 00 02 00 00 00 00 08 00 00	?...0.....
00000210h:	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0@..?
00000220h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000230h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000240h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000250h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000260h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000270h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000280h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000290h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

DOS 桩

0 1 2 3 4 5 6 7 8 9 A B C D E F

000002a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000300h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000310h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000330h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000340h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000350h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000360h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000370h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000380h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000390h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000400h:	68 40 10 00 00 68 00 30 40 00 68 09 30 40 00 6A	h@...h.0@.h.0@.j
00000410h:	00 E8 2A 00 00 00 68 40 10 00 00 68 00 30 40 00	.?...h@...h.0@.
00000420h:	68 31 30 40 00 6A 00 E8 14 00 00 6A 00 E8 01	h10@.j.?...j.?
00000430h:	00 00 00 CC FF 25 00 20 40 00 FF 25 0C 20 40 00	...?%. @. %. @.
00000440h:	FF 25 08 20 40 00 00 00 00 00 00 00 00 00 00 00	%. @.....
00000450h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000460h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000470h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000480h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000490h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004a0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004b0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004c0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004e0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000500h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000510h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000520h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000530h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000540h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000550h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000560h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000570h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000580h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

节表

(本例包含代码节、引入函数节、数据节3个表项, 每表项20字节)

- 节名称(.text)
- 节的RVA
- 节的长度
- 节在文件中的位置
- 节属性

代码节