PE 文件结构解析作业

1. 已知某 PE 文件头如下图所示，请解析

Machine 、 NumberOfSections 、 SizeOfOptionalHeader 、 SizeOfCode 、 AddressOfEntryPoint、 SectionAlignment、 FileAlignment、 SizeOfImage、 SizeOfHeaders 的值。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00
00000080	58	0A	22	8D	1C	6B	4C	DE	1C	6B	4C	DE	1C	6B	4C	DE
00000090	C9	06	4D	DF	1F	6B	4C	DE	C9	06	49	DF	05	6B	4C	DE
000000A0	C9	06	48	DF	11	6B	4C	DE	47	03	4D	DF	18	6B	4C	DE
000000B0	1C	6B	4D	DE	58	6B	4C	DE	80	05	49	DF	1D	6B	4C	DE
000000C0	80	05	B3	DE	1D	6B	4C	DE	80	05	4E	DF	1D	6B	4C	DE
000000D0	52	69	63	68	1C	6B	4C	DE	00	00	00	00	00	00	00	00
000000E0	50	45	00	00	4C	01	09	00	E6	FA	82	5F	00	00	00	00
000000F0	00	00	00	00	E0	00	02	01	0B	01	0E	18	00	54	00	00
00000100	00	44	00	00	00	00	00	00	3E	13	01	00	00	10	00	00
00000110	00	10	00	00	00	00	40	00	00	10	00	00	00	02	00	00
00000120	06	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00
00000130	00	00	02	00	00	04	00	00	00	00	00	00	03	00	40	81
00000140	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00
00000150	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000160	C4	B1	01	00	50	00	00	00	00	E0	01	00	3C	04	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	F0	01	00	70	03	00	00	F0	84	01	00	38	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	28	85	01	00	40	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	B0	01	00	C4	01	00	00

名字	Value
Machine	0x014C
NumberOfSections	0x0009
SizeOfOptionalHeader	0x00E0
SizeOfCode	0x00005400
AddressOfEntryPoint	0x0001133E
SectionAlignment	0x00001000
FileAlignment	0x00000200
SizeOfImage	0x00020000
SizeOfHeaders	0x00000400

2. 已知某 PE 文件的节表如下图所示，请解析节表中每个节的 Name、VirtualSize、VirtualAddress 、 SizeOfRawData 、 PointerToRawData 。

```
00000200  2E 74 65 78 74 00 00 00  C4 53 00 00 00 10 01 00
00000210  00 54 00 00 00 04 00 00  00 00 00 00 00 00 00 00
00000220  00 00 00 00 20 00 00 60  2E 72 64 61 74 61 00 00
00000230  11 20 00 00 00 70 01 00  00 22 00 00 00 58 00 00
00000240  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 40
00000250  2E 64 61 74 61 00 00 00  98 05 00 00 00 A0 01 00
00000260  00 02 00 00 00 7A 00 00  00 00 00 00 00 00 00 00
00000270  00 00 00 00 40 00 00 C0  2E 69 64 61 74 61 00 00
00000280  DE 0A 00 00 00 B0 01 00  00 0C 00 00 00 7C 00 00
00000290  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 40
000002A0  2E 6D 73 76 63 6A 6D 63  06 01 00 00 00 C0 01 00
000002B0  00 02 00 00 00 88 00 00  00 00 00 00 00 00 00 00
000002C0  00 00 00 00 40 00 00 C0  2E 30 30 63 66 67 00 00
000002D0  04 01 00 00 00 D0 01 00  00 02 00 00 00 8A 00 00
000002E0  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 40
000002F0  2E 72 73 72 63 00 00 00  3C 04 00 00 00 E0 01 00
00000300  00 06 00 00 00 8C 00 00  00 00 00 00 00 00 00 00
00000310  00 00 00 00 40 00 00 40  2E 72 65 6C 6F 63 00 00
00000320  63 05 00 00 00 F0 01 00  00 06 00 00 00 92 00 00
00000330  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 42
```

名字	Value
Name	.text
VirtualSize	0x0110
VirtualAddress	0x53c4
SizeOfRawData	0x5400
PointerToRawData	0x0400
名字	**Value**
Name	.rdata
VirtualSize	0x0170
VirtualAddress	0x2011
SizeOfRawData	0x2200
PointerToRawData	0x5800
名字	**Value**
Name	.data
VirtualSize	0x01A0
VirtualAddress	0x0598
SizeOfRawData	0x2200
PointerToRawData	0x7A00
名字	**Value**
Name	.idata
VirtualSize	0x01B0
VirtualAddress	0x0ADE
SizeOfRawData	0x0C00

PointerToRawData	0x7C00
名字	**Value**
Name	.msvcjmc
VirtualSize	0x01c0
VirtualAddress	0x0106
SizeOfRawData	0x8800
PointerToRawData	0x4000
名字	**Value**
Name	.00cfg
VirtualSize	0x01D0
VirtualAddress	0x0104
SizeOfRawData	0x0200
PointerToRawData	0x8A00
名字	**Value**
Name	.rsrc
VirtualSize	0x01E0
VirtualAddress	0x043C
SizeOfRawData	0x0600
PointerToRawData	0x8C00
名字	**Value**
Name	.reloc
VirtualSize	0x01F0
VirtualAddress	0x0563
SizeOfRawData	0x0600
PointerToRawData	0x9200

以下三道题看 PE 的 pdf

3．请解析 USER32.DLL 前 5 个导出函数的信息，要求列举 AddressOfNams、AddressOfOrdinals、AddressOfFunctions 的详细数据。

4．编写程序并生成 exe 文件，要求定义 1048 个字节长度的 word 数组，在程序中对该数组赋随机数，然后查找该数组的最小值，并调用 MessageBox 函数和 ExitProcess 函数。

5．请解析题 4 生成 exe 文件的节表，加载前、后导入函数的详细信息。