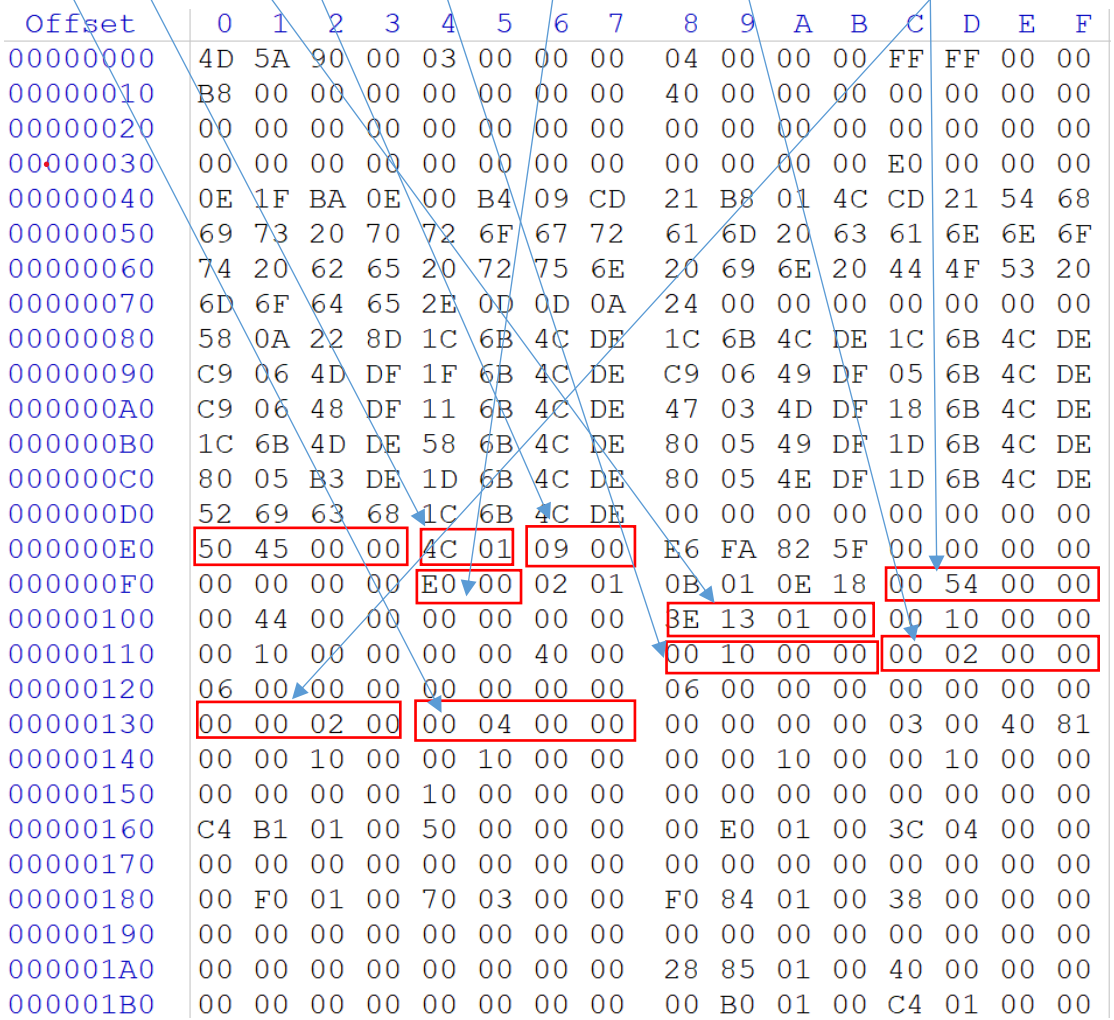
20214816 刘静婷 信息安全 1 班

PE 文件结构解析作业一

1. 已知某 PE 文件头如下图所示，请解析

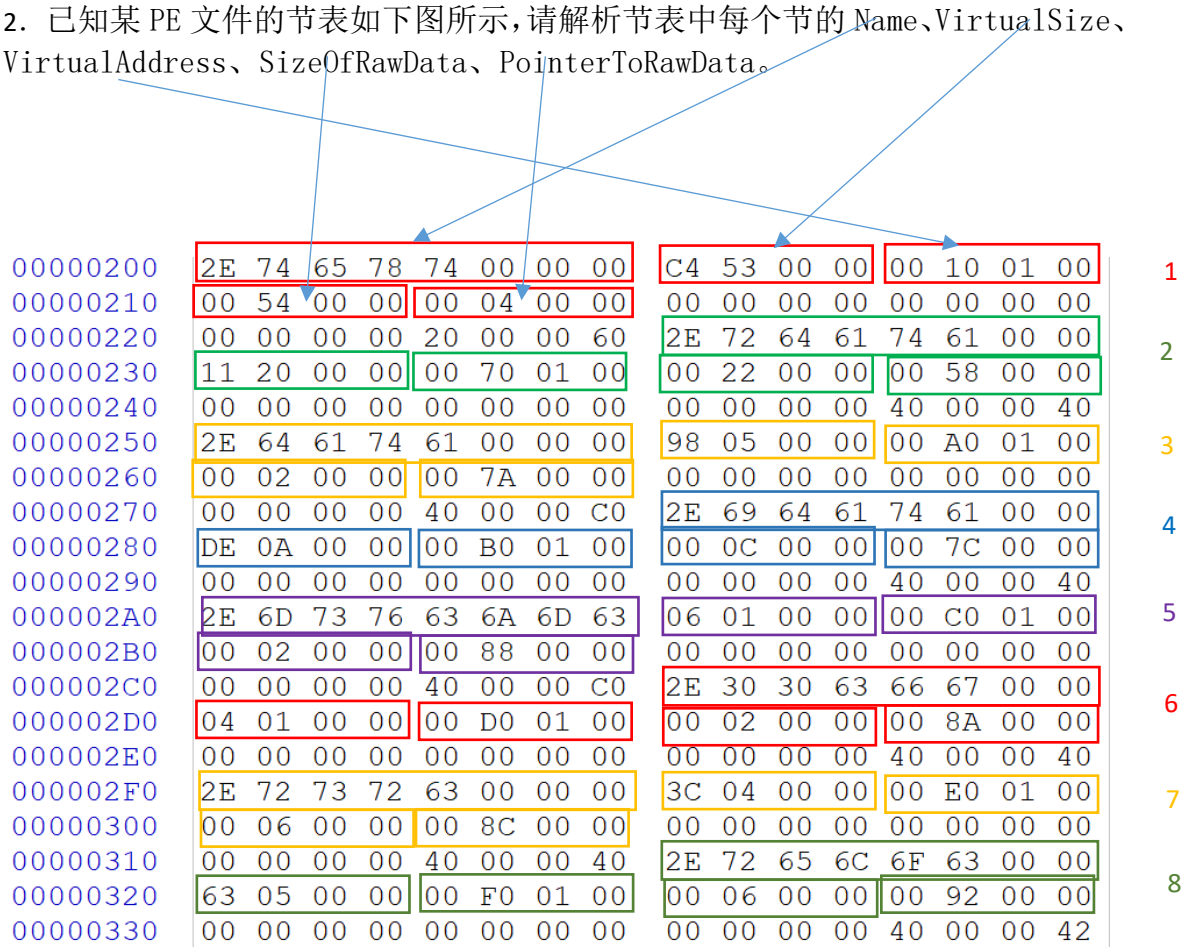
Machine 、 NumberOfSections 、 SizeOfOptionalHeader 、 SizeOfCode 、 AddressOfEntryPoint、 SectionAlignment、 FileAlignment、 SizeOfImage、 SizeOfHeaders 的值。



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

Machine	014C
NumberOfSections	0009
SizeOfOptionalHeader	00E0
SizeOfCode	00005400
AddressOfEntryPoint	0001133E
SectionAlignment	00001000
FileAlignment	00000200
SizeOfImage	00020000
SizeOfHeaders	00000400

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。



Name	000000747865742E
VirtualSize	000053C4
VirtualAddress	00011000
SizeOfRawData	00005400
PointerToRawData	00000400

Name	000061746164722E
VirtualSize	00002011
VirtualAddress	00017000
SizeOfRawData	00002200
PointerToRawData	00005800

Name	000000617461642E
VirtualSize	00000598
VirtualAddress	0001A000
SizeOfRawData	00000200
PointerToRawData	00007A00

Name	000061746164692E
VirtualSize	00000ADE
VirtualAddress	0001B000
SizeOfRawData	00000C00
PointerToRawData	00007C00

Name	636D6A6376736D2E
VirtualSize	00000106
VirtualAddress	0001C000
SizeOfRawData	00000200
PointerToRawData	00008800

Name	000067666330302E
VirtualSize	00000104
VirtualAddress	0001D000
SizeOfRawData	00000200
PointerToRawData	00008A00

Name	000000637273722E
VirtualSize	0000043C
VirtualAddress	0001E000
SizeOfRawData	00000600
PointerToRawData	00008C00

Name	0000636F6C65722E
VirtualSize	0000563
VirtualAddress	0001F000
SizeOfRawData	00000600
PointerToRawData	00009200