Formatul Portable Executable

Training Bitdefender Cluj-Napoca

Ciprian Oprișa

Bitdefender

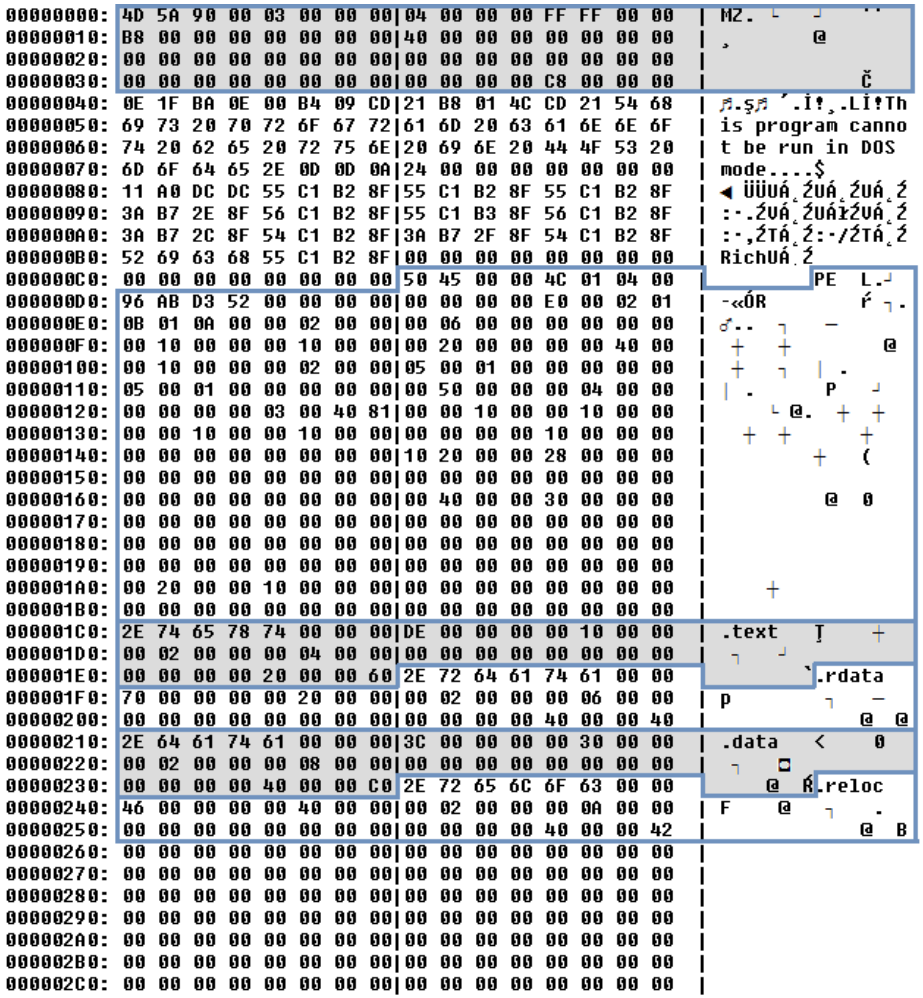
27 octombrie 2018

Cuprins

Cuprins

Ce se vede cu ochiul liber

Delimitarea header-elor



Bitdefender

Cuprins

Image DOS Header

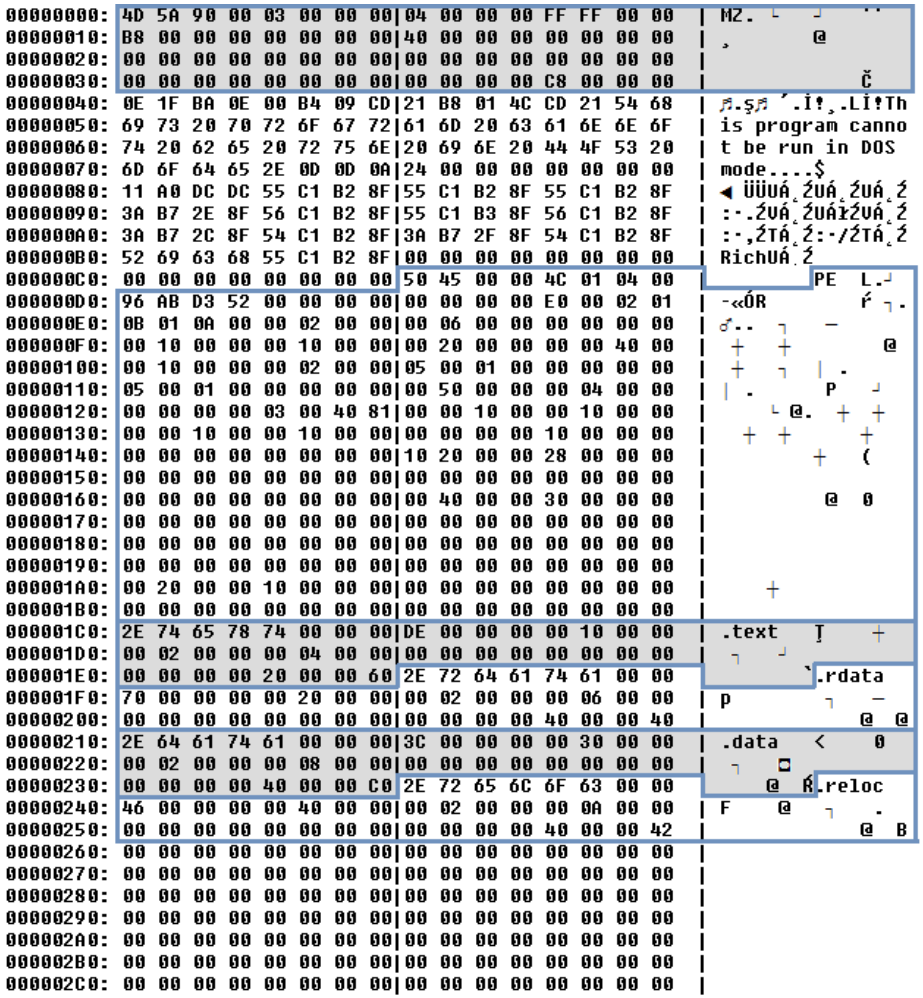
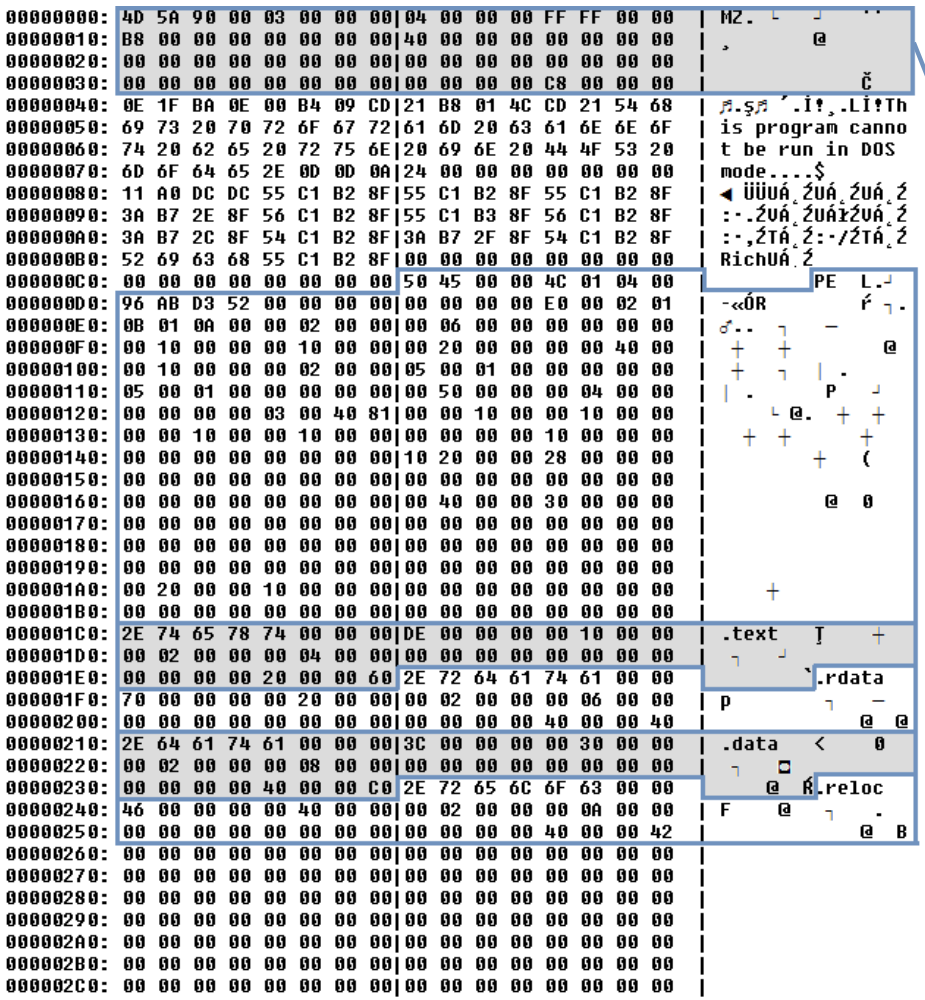
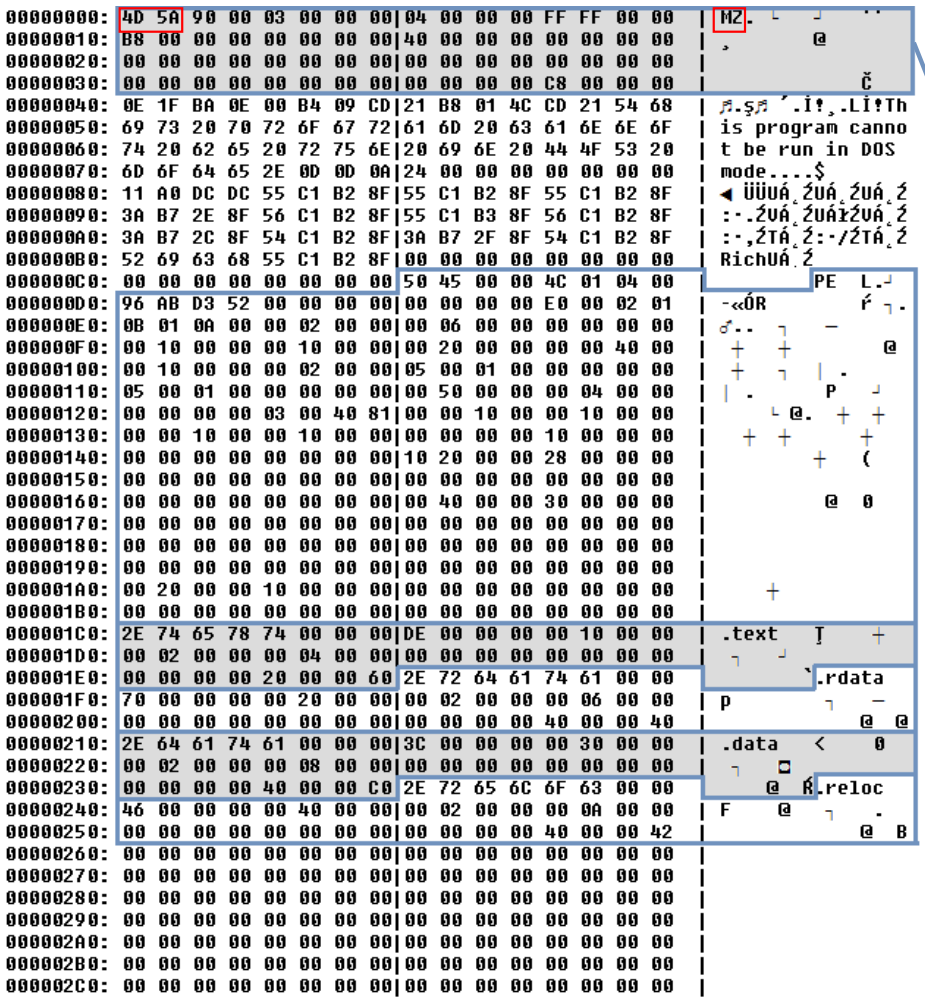


Image DOS Header



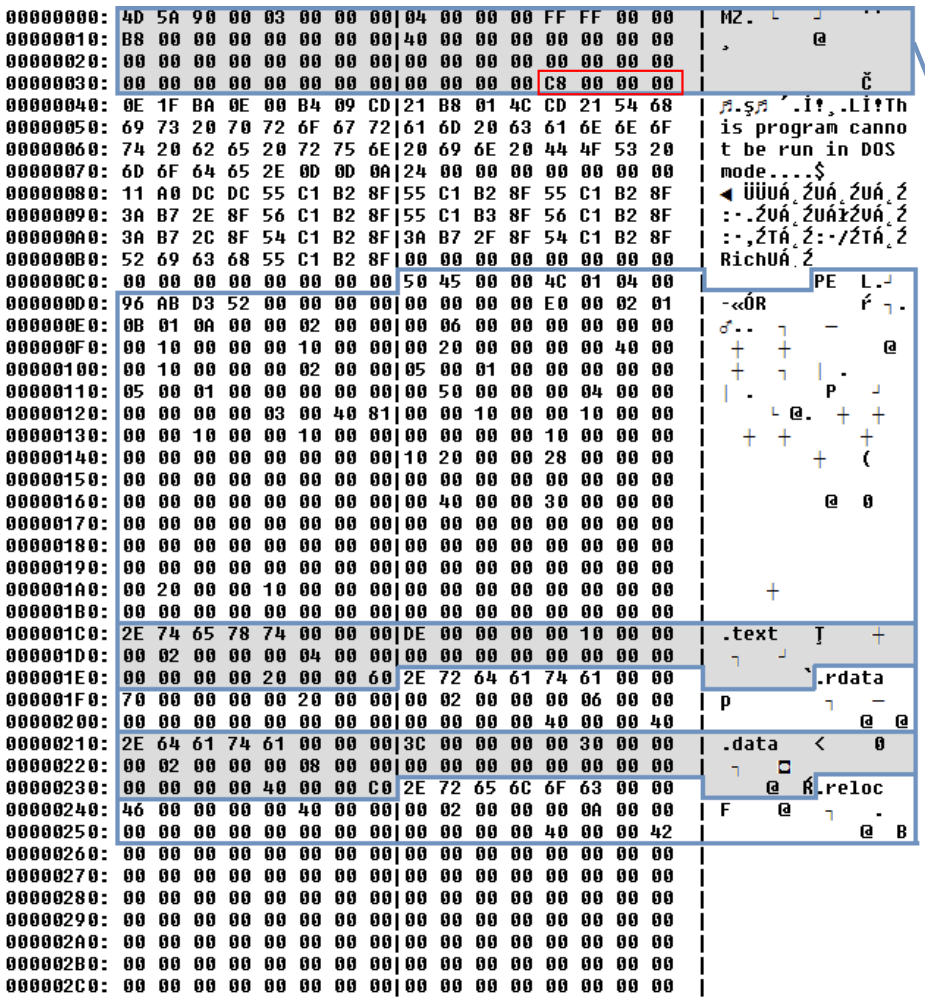

```
struct _IMAGE_DOS_HEADER {
0x00  WORD e_magic;
0x02  WORD e_cblp;
0x04  WORD e_cp;
0x06  WORD e_crlc;
0x08  WORD e_cparhdr;
0x0a  WORD e_minalloc;
0x0c  WORD e_maxalloc;
0x0e  WORD e_ss;
0x10  WORD e_sp;
0x12  WORD e_csum;
0x14  WORD e_ip;
0x16  WORD e_cs;
0x18  WORD e_lfarlc;
0x1a  WORD e_ovno;
0x1c  WORD e_res[4];
0x24  WORD e_oemid;
0x26  WORD e_oeminfo;
0x28  WORD e_res2[10];
0x3c  DWORD e_lfanew;
};
```

Image DOS Header



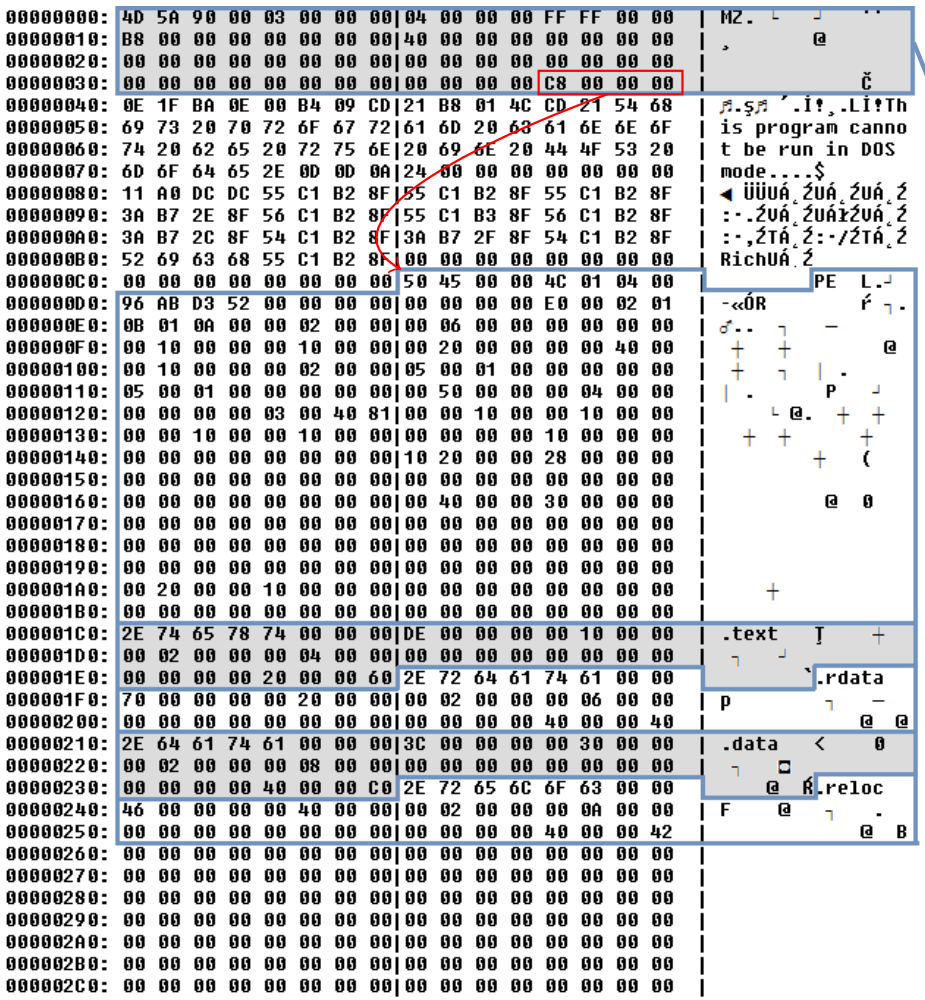

```
struct _IMAGE_DOS_HEADER {
0x00  WORD e_magic;
0x02  WORD e_cblp;
0x04  WORD e_cp;
0x06  WORD e_crlc;
0x08  WORD e_cparhdr;
0x0a  WORD e_minalloc;
0x0c  WORD e_maxalloc;
0x0e  WORD e_ss;
0x10  WORD e_sp;
0x12  WORD e_csum;
0x14  WORD e_ip;
0x16  WORD e_cs;
0x18  WORD e_lfarlc;
0x1a  WORD e_ovno;
0x1c  WORD e_res[4];
0x24  WORD e_oemid;
0x26  WORD e_oeminfo;
0x28  WORD e_res2[10];
0x3c  DWORD e_lfanew;
};
```

Image DOS Header




```
struct _IMAGE_DOS_HEADER {
0x00   WORD e_magic;
0x02   WORD e_cblp;
0x04   WORD e_cp;
0x06   WORD e_crlc;
0x08   WORD e_cparhdr;
0x0a   WORD e_minalloc;
0x0c   WORD e_maxalloc;
0x0e   WORD e_ss;
0x10   WORD e_sp;
0x12   WORD e_csum;
0x14   WORD e_ip;
0x16   WORD e_cs;
0x18   WORD e_lfarlc;
0x1a   WORD e_ovno;
0x1c   WORD e_res[4];
0x24   WORD e_oemid;
0x26   WORD e_oeminfo;
0x28   WORD e_res2[10];
0x3c   DWORD e_lfanew;
};
```

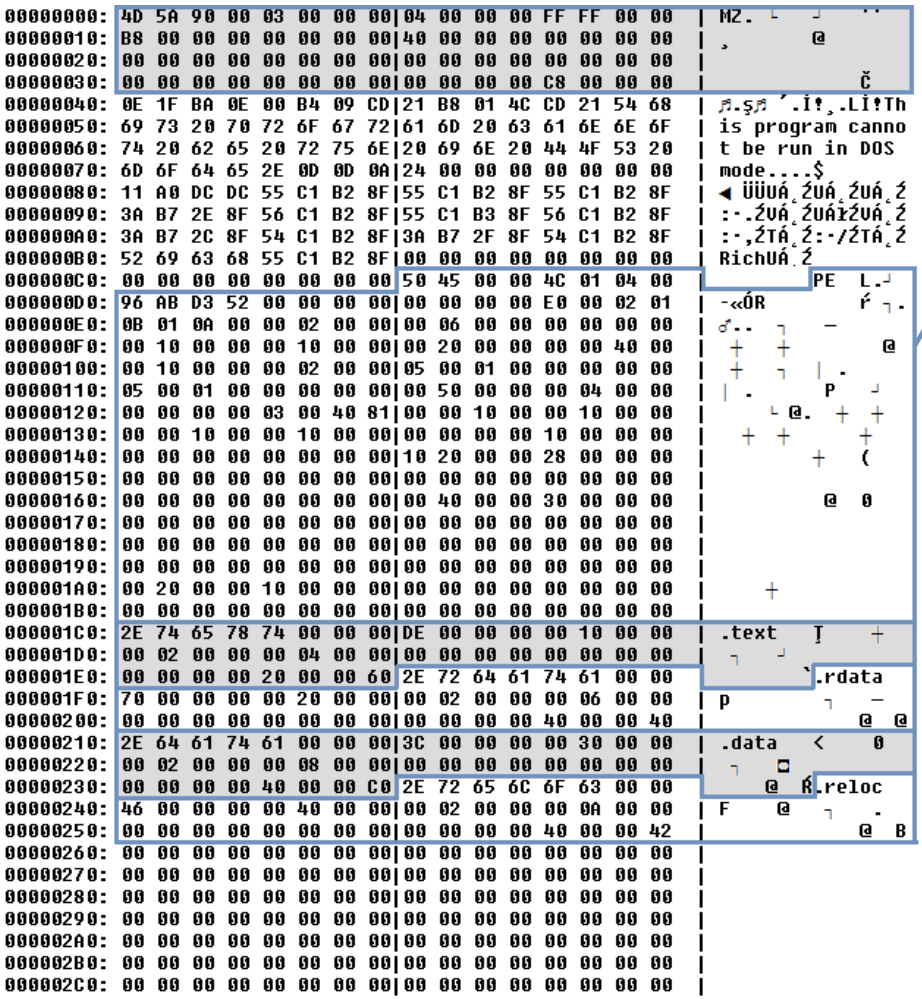
Image DOS Header




```
struct _IMAGE_DOS_HEADER {
0x00   WORD e_magic;
0x02   WORD e_cblp;
0x04   WORD e_cp;
0x06   WORD e_crlc;
0x08   WORD e_cparhdr;
0x0a   WORD e_minalloc;
0x0c   WORD e_maxalloc;
0x0e   WORD e_ss;
0x10   WORD e_sp;
0x12   WORD e_csum;
0x14   WORD e_ip;
0x16   WORD e_cs;
0x18   WORD e_lfarlc;
0x1a   WORD e_ovno;
0x1c   WORD e_res[4];
0x24   WORD e_oemid;
0x26   WORD e_oeminfo;
0x28   WORD e_res2[10];
0x3c   DWORD e_lfanew;
};
```

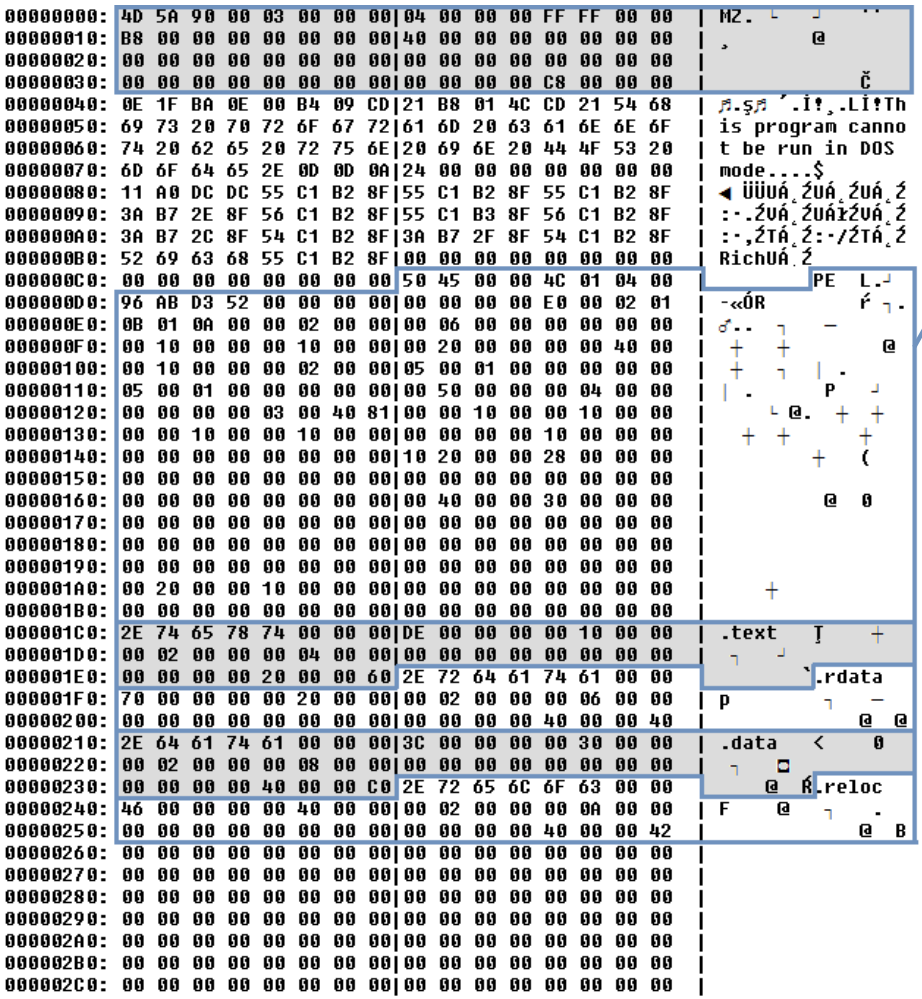
Cuprins

Image NT Headers




```
struct _IMAGE_NT_HEADERS {
0x00  DWORD Signature;
0x04  _IMAGE_FILE_HEADER FileHeader;
0x18  _IMAGE_OPTIONAL_HEADER OptionalHeader;
};
```

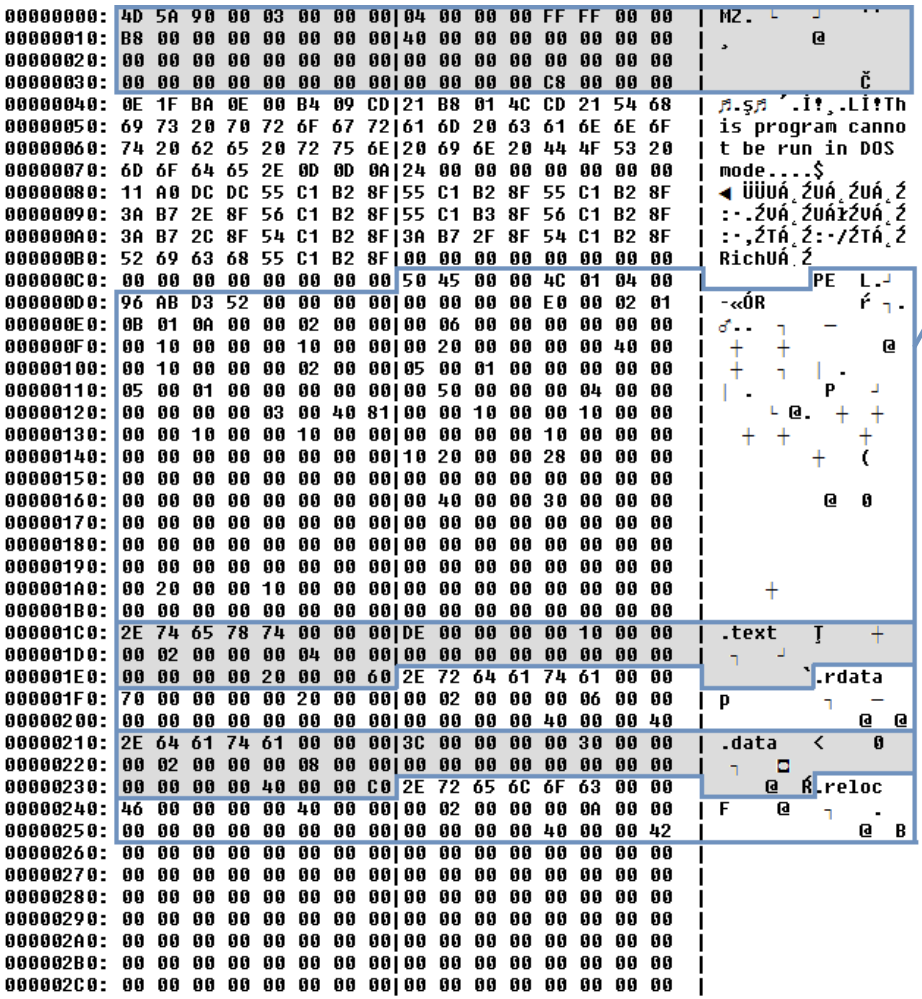
Image NT Headers



struct _IMAGE_NT_HEADERS {
0x00 DWORD Signature;
0x04 _IMAGE_FILE_HEADER FileHeader;
0x18 _IMAGE_OPTIONAL_HEADER OptionalHeader;
};

struct _IMAGE_FILE_HEADER {
0x00 WORD Machine;
0x02 WORD NumberOfSections;
0x04 DWORD TimeDateStamp;
0x08 DWORD PointerToSymbolTable;
0x0c DWORD NumberOfSymbols;
0x10 WORD SizeOfOptionalHeader;
0x12 WORD Characteristics;
};

Image NT Headers




```
struct _IMAGE_NT_HEADERS {
0x00  DWORD Signature;
0x04  _IMAGE_FILE_HEADER FileHeader;
0x18  _IMAGE_OPTIONAL_HEADER OptionalHeader;
};
```

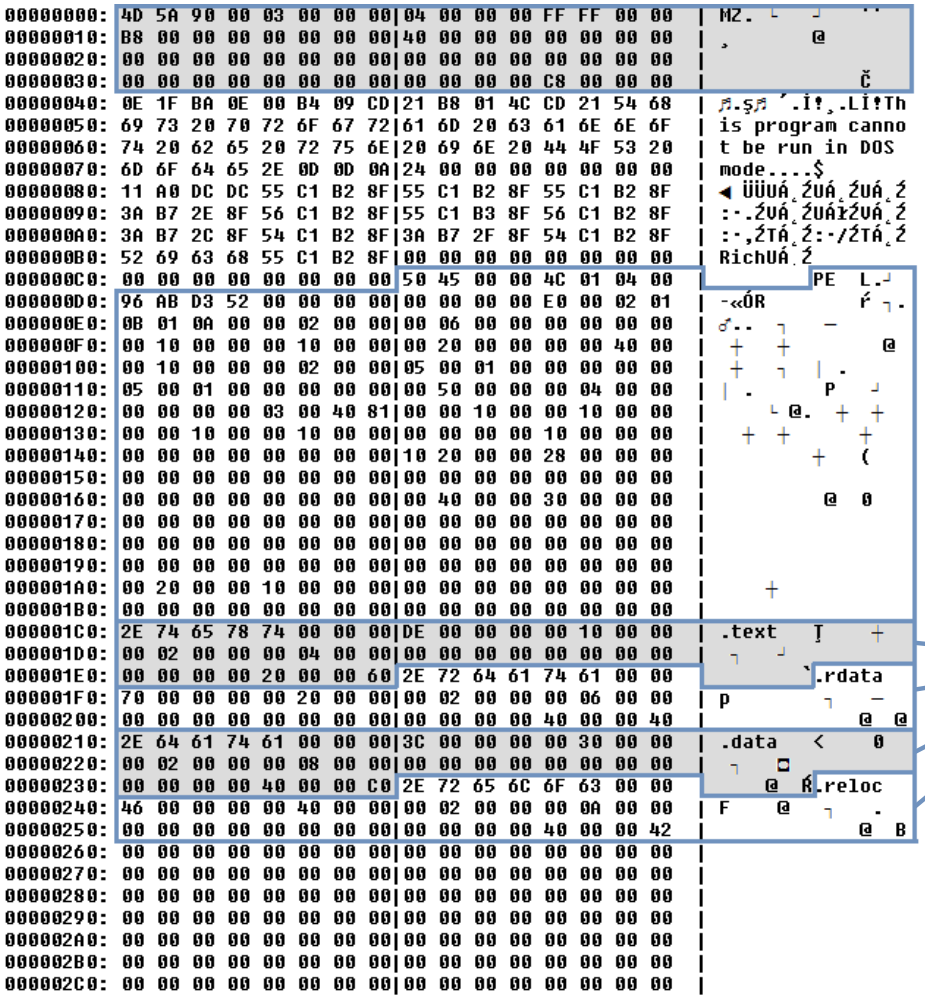
```
struct _IMAGE_FILE_HEADER {
0x00  WORD Machine;
0x02  WORD NumberOfSections;
0x04  DWORD TimeDateStamp;
0x08  DWORD PointerToSymbolTable;
0x0c  DWORD NumberOfSymbols;
0x10  WORD SizeOfOptionalHeader;
0x12  WORD Characteristics;
};
```

```
struct _IMAGE_OPTIONAL_HEADER {
0x00  WORD Magic;
0x02  BYTE MajorLinkerVersion;
0x03  BYTE MinorLinkerVersion;
0x04  DWORD SizeOfCode;
0x08  DWORD SizeOfInitializedData;
0x0c  DWORD SizeOfUninitializedData;
0x10  DWORD AddressOfEntryPoint;
0x14  DWORD BaseOfCode;
0x18  DWORD BaseOfData;
0x1c  DWORD ImageBase;
0x20  DWORD SectionAlignment;
0x24  DWORD FileAlignment;
0x28  WORD MajorOperatingSystemVersion;
0x2a  WORD MinorOperatingSystemVersion;
0x2c  WORD MajorImageVersion;
0x2e  WORD MinorImageVersion;
0x30  WORD MajorSubsystemVersion;
0x32  WORD MinorSubsystemVersion;
0x34  DWORD Win32VersionValue;
0x38  DWORD SizeOfImage;
0x3c  DWORD SizeOfHeaders;
0x40  DWORD CheckSum;
0x44  WORD Subsystem;
0x46  WORD DllCharacteristics;
0x48  DWORD SizeOfStackReserve;
0x4c  DWORD SizeOfStackCommit;
0x50  DWORD SizeOfHeapReserve;
0x54  DWORD SizeOfHeapCommit;
0x58  DWORD LoaderFlags;
0x5c  DWORD NumberOfRvaAndSizes;
0x60  _IMAGE_DATA_DIRECTORY DataDirectory[16];
};
```

Bitdefender

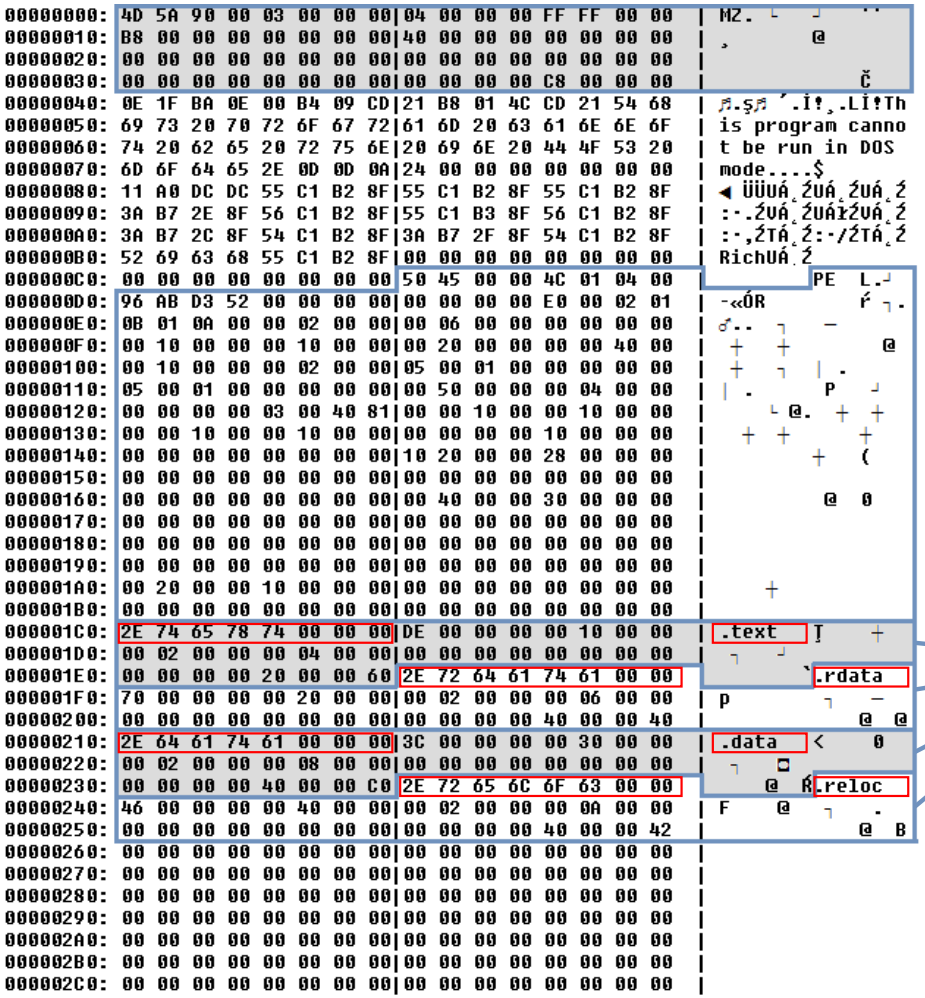
Cuprins

Image Section Headers (1)



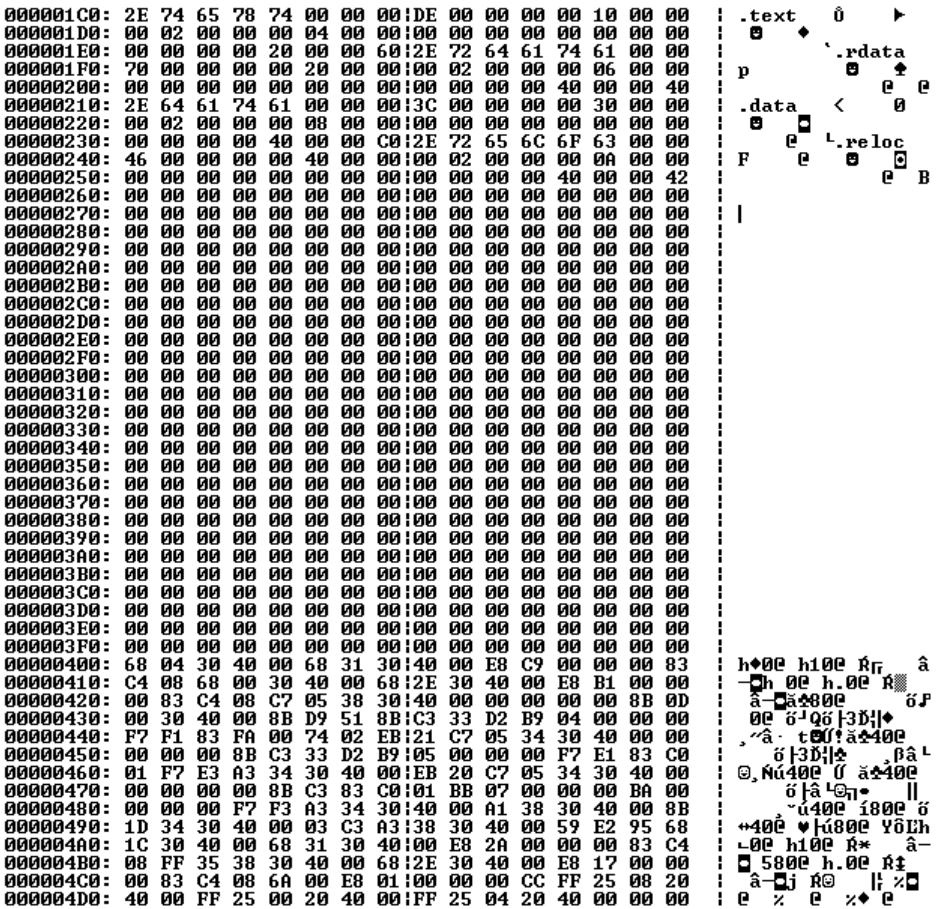

```
typedef struct _IMAGE_SECTION_HEADER {
0x00  BYTE  Name[IMAGE_SIZEOF_SHORT_NAME];
      union {
0x08          DWORD PhysicalAddress;
0x08          DWORD VirtualSize;
      } Misc;
0x0c  DWORD VirtualAddress;
0x10  DWORD SizeOfRawData;
0x14  DWORD PointerToRawData;
0x18  DWORD PointerToRelocations;
0x1c  DWORD PointerToLinenumbers;
0x20  WORD  NumberOfRelocations;
0x22  WORD  NumberOfLinenumbers;
0x24  DWORD Characteristics;
};
```

Image Section Headers (1)




```
typedef struct _IMAGE_SECTION_HEADER {
0x00  BYTE  Name[IMAGE_SIZEOF_SHORT_NAME];
      union {
0x08          DWORD PhysicalAddress;
0x08          DWORD VirtualSize;
      } Misc;
0x0c  DWORD VirtualAddress;
0x10  DWORD SizeOfRawData;
0x14  DWORD PointerToRawData;
0x18  DWORD PointerToRelocations;
0x1c  DWORD PointerToLinenumbers;
0x20  WORD  NumberOfRelocations;
0x22  WORD  NumberOfLinenumbers;
0x24  DWORD Characteristics;
};
```

Image Section Headers (2)



```
000001C0: 2E 74 65 78 74 00 00 00:DE 00 00 00 00 10 00 00  | .text    Û      ►
000001D0: 00 02 00 00 00 04 00 00:00 00 00 00 00 00 00 00  |  ☻    ♦
000001E0: 00 00 00 00 20 00 00 60:2E 72 64 61 74 61 00 00  |          `.rdata
000001F0: 70 00 00 00 00 20 00 00:00 02 00 00 00 06 00 00  | p        ☻     ♠
00000200: 00 00 00 00 00 00 00 00:00 00 00 00 40 00 00 40  |                @  @
00000210: 2E 64 61 74 61 00 00 00:3C 00 00 00 00 30 00 00  | .data    <     0
00000220: 00 02 00 00 00 08 00 00:00 00 00 00 00 00 00 00  |  ☻     ◘
00000230: 00 00 00 00 40 00 00 C0:2E 72 65 6C 6F 63 00 00  |     @   └.reloc
00000240: 46 00 00 00 00 40 00 00:00 02 00 00 00 0A 00 00  | F     @     ☻     ◙
00000250: 00 00 00 00 00 00 00 00:00 00 00 00 40 00 00 42  |                @  B
00000260: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000270: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000280: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000290: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002A0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002B0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002C0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002D0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002E0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002F0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000300: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000310: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000320: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000330: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000340: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000350: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000360: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000370: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000380: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000390: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003A0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003B0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003C0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003D0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003E0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003F0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000400: 68 04 30 40 00 68 31 30:40 00 E8 C9 00 00 00 83  | h♦0@ h10@ Ŕ╔   â
00000410: C4 08 68 00 30 40 00 68:2E 30 40 00 E8 B1 00 00  | ─◘h 0@ h.0@ Ř▒
00000420: 00 83 C4 08 C7 05 38 30:40 00 00 00 00 00 8B 0D  |  â─◘ă♣80@      ő♪
00000430: 00 30 40 00 8B D9 51 8B:C3 33 D2 B9 04 00 00 00  |  0@ ő┘Qő├3Ď╣♦
00000440: F7 F1 83 FA 00 74 02 EB:21 C7 05 34 30 40 00 00  | ╖±â· t☻Ű!ă♣40@
00000450: 00 00 00 8B C3 33 D2 B9:05 00 00 00 F7 E1 83 C0  |    ő├3Ď╣♣      ╖ßâ└
00000460: 01 F7 E3 A3 34 30 40 00:EB 20 C7 05 34 30 40 00  | ☺╖Ńú40@ Ű ă♣40@
00000470: 00 00 00 00 8B C3 83 C0:01 BB 07 00 00 00 BA 00  |     ő├â└☺╗•    ||
00000480: 00 00 00 F7 F3 A3 34 30:40 00 A1 38 30 40 00 8B  |     ˘ú40@ í80@ ő
00000490: 1D 34 30 40 00 03 C3 A3:38 30 40 00 59 E2 95 68  | ↔40@ ♥├ú80@ YôĽh
000004A0: 1C 30 40 00 68 31 30 40:00 E8 2A 00 00 00 83 C4  | └0@ h10@ Ř*   â─
000004B0: 08 FF 35 38 30 40 00 68:2E 30 40 00 E8 17 00 00  | ◘ 580@ h.0@ Ř↨
000004C0: 00 83 C4 08 6A 00 E8 01:00 00 00 CC FF 25 08 20  |  â─◘j Ř☺    ╠ ˙%◘
000004D0: 40 00 FF 25 00 20 40 00:FF 25 04 20 40 00 00 00  | @  ˙  @  ˙♦ @
```

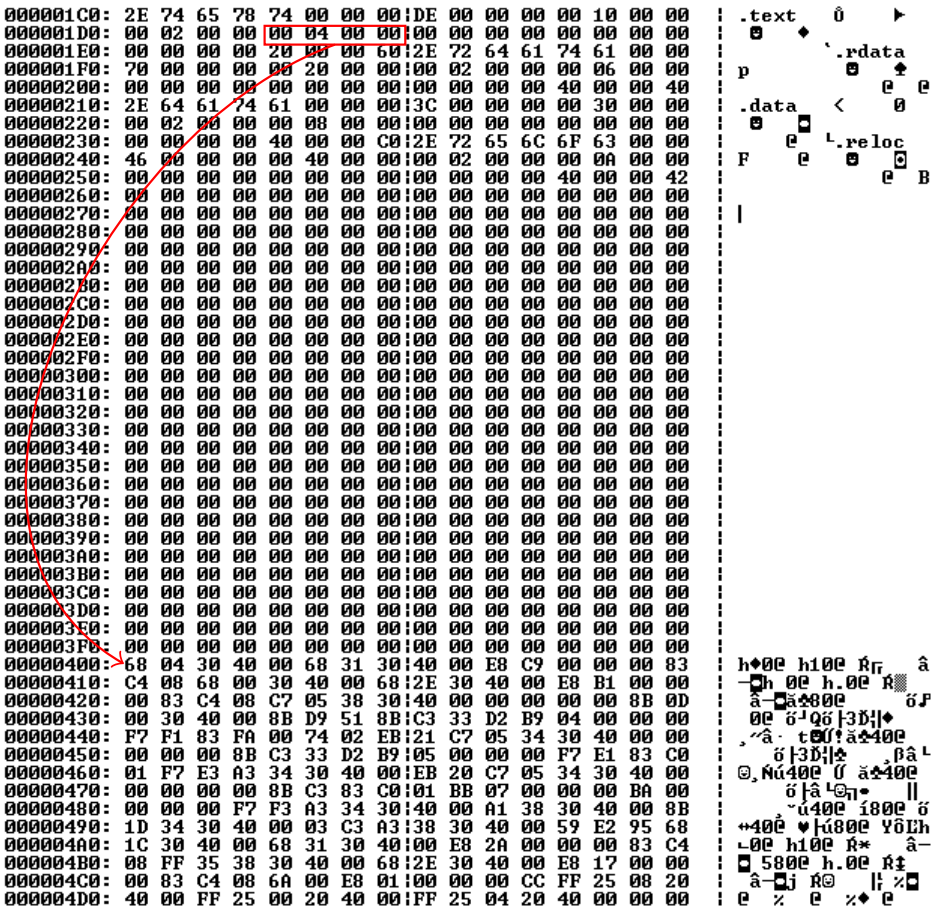
```
typedef struct _IMAGE_SECTION_HEADER {
0x00  BYTE  Name[IMAGE_SIZEOF_SHORT_NAME];
      union {
0x08        DWORD PhysicalAddress;
0x08        DWORD VirtualSize;
      } Misc;
0x0c  DWORD VirtualAddress;
0x10  DWORD SizeOfRawData;
0x14  DWORD PointerToRawData;
0x18  DWORD PointerToRelocations;
0x1c  DWORD PointerToLinenumbers;
0x20  WORD  NumberOfRelocations;
0x22  WORD  NumberOfLinenumbers;
0x24  DWORD Characteristics;
};
```

Image Section Headers (2)

```
000001C0: 2E 74 65 78 74 00 00 00:DE 00 00 00 00 10 00 00  | .text    Þ      ►
000001D0: 00 02 00 00 00 04 00 00:00 00 00 00 00 00 00 00  |  ☻    ♦
000001E0: 00 00 00 00 20 00 00 60:2E 72 64 61 74 61 00 00  |          `.rdata
000001F0: 70 00 00 00 00 20 00 00:00 02 00 00 00 06 00 00  | p        ☻     ♠
00000200: 00 00 00 00 00 00 00 00:00 00 00 00 40 00 00 40  |                @  @
00000210: 2E 64 61 74 61 00 00 00:3C 00 00 00 00 30 00 00  | .data    <     0
00000220: 00 02 00 00 00 08 00 00:00 00 00 00 00 00 00 00  |  ☻     ◘
00000230: 00 00 00 00 40 00 00 C0:2E 72 65 6C 6F 63 00 00  |     @   └.reloc
00000240: 46 00 00 00 00 40 00 00:00 02 00 00 00 0A 00 00  | F     @     ☻     ◙
00000250: 00 00 00 00 00 00 00 00:00 00 00 00 40 00 00 42  |                @  B
00000260: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000270: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000280: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000290: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002A0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002B0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002C0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002D0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002E0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000002F0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000300: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000310: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000320: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000330: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000340: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000350: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000360: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000370: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000380: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000390: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003A0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003B0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003C0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003D0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003E0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
000003F0: 00 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00  |
00000400: 68 04 30 40 00 68 31 30:40 00 E8 C9 00 00 00 83  | h♦0@ h10@ Ŕ╔   â
00000410: C4 08 68 00 30 40 00 68:2E 30 40 00 E8 B1 00 00  | ─◘h 0@ h.0@ Ŕ▒
00000420: 00 83 C4 08 C7 05 38 30:40 00 00 00 00 00 8B 0D  |  â─◘ă♣80@      ő♪
00000430: 00 30 40 00 8B D9 51 8B:C3 33 D2 B9 04 00 00 00  |  0@ ő┘Qő├3Ď╣♦
00000440: F7 F1 83 FA 00 74 02 EB:21 C7 05 34 30 40 00 00  | ╖±â· t☻Ű!ă♣40@
00000450: 00 00 00 8B C3 33 D2 B9:05 00 00 00 F7 E1 83 C0  |    ő├3Ď╣♣    ╖ßâ└
00000460: 01 F7 E3 A3 34 30 40 00:EB 20 C7 05 34 30 40 00  | ☺ Ńú40@ Ű ă♣40@
00000470: 00 00 00 00 8B C3 83 C0:01 BB 07 00 00 00 BA 00  |     ő├â└☺╗•    ||
00000480: 00 00 00 F7 F3 A3 34 30:40 00 A1 38 30 40 00 8B  |     ˘ú40@ í80@ ő
00000490: 1D 34 30 40 00 03 C3 A3:38 30 40 00 59 E2 95 68  | ↔40@ ♥├ú80@ YôĽh
000004A0: 1C 30 40 00 68 31 30 40:00 E8 2A 00 00 00 83 C4  | └0@ h10@ Ŕ*   â─
000004B0: 08 FF 35 38 30 40 00 68:2E 30 40 00 E8 17 00 00  | ◘ 580@ h.0@ Ŕ↨
000004C0: 00 83 C4 08 6A 00 E8 01:00 00 00 CC FF 25 08 20  |  â─◘j Ŕ☺    ╠ ˙% ◘
000004D0: 40 00 FF 25 00 20 40 00:FF 25 04 20 40 00 00 00  | @  %  @  %♦ @
```

```
typedef struct _IMAGE_SECTION_HEADER {
0x00  BYTE  Name[IMAGE_SIZEOF_SHORT_NAME];
      union {
0x08          DWORD PhysicalAddress;
0x08          DWORD VirtualSize;
      } Misc;
0x0c  DWORD VirtualAddress;
0x10  DWORD SizeOfRawData;
0x14  DWORD PointerToRawData;
0x18  DWORD PointerToRelocations;
0x1c  DWORD PointerToLinenumbers;
0x20  WORD  NumberOfRelocations;
0x22  WORD  NumberOfLinenumbers;
0x24  DWORD Characteristics;
};
```

Image Section Headers (2)




```
typedef struct _IMAGE_SECTION_HEADER {
0x00  BYTE  Name[IMAGE_SIZEOF_SHORT_NAME];
      union {
0x08        DWORD PhysicalAddress;
0x08        DWORD VirtualSize;
      } Misc;
0x0c  DWORD VirtualAddress;
0x10  DWORD SizeOfRawData;
0x14  DWORD PointerToRawData;
0x18  DWORD PointerToRelocations;
0x1c  DWORD PointerToLinenumbers;
0x20  WORD  NumberOfRelocations;
0x22  WORD  NumberOfLinenumbers;
0x24  DWORD Characteristics;
};
```