

# Formatul Portable Executable

## Training Bitdefender Cluj-Napoca

Ciprian Oprea

Bitdefender

27 octombrie 2018

# Cuprins

- 1 Header-ele unui executabil
- 2 Image DOS Header
- 3 Image NT Headers
- 4 Header-ele secțiunilor

# Cuprins

- 1 Header-ele unui executabil
- 2 Image DOS Header
- 3 Image NT Headers
- 4 Header-ele secțiunilor

# Ce se vede cu ochiul liber

```

00000000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ. . . .
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 00 C8 00 00 00 | .C
00000040: 0E 1F BA 0E 0A B4 09 CD 21 B8 01 4C CD 21 54 68 | .!$%&'()*+,-./:;@A[B\]^_`{|}~
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F | is program cannot
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS
00000070: 6D 6F 64 65 2E 00 00 00 0A 24 00 00 00 00 00 00 | mode...$
00000080: 11 00 DC DC 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F | 4 UUUA, 20A, 20A, 2
00000090: 30 B7 2E 8F 54 C1 B2 8F 55 C1 B2 8F 54 C1 B2 8F | :- 20A, 20A, 20A, 2
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F | :- 21A, 21A, 21A, 2
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 | RichUA, 2
000000C0: 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE L.
000000D0: 96 0B D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 | -dOR f.
000000E0: 0B 01 0A 00 00 00 02 00 00 00 06 00 00 00 00 00 | . . . -
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00 | + + @
00000100: 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 | + + |
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 04 00 00 00 | | . P
00000120: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 | | . @. + +
00000130: 00 00 10 00 00 10 00 00 00 00 10 00 00 00 00 00 | + + +
00000140: 00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 | + + (
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | @ @
00000160: 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 00 |
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
000001C0: 2E 74 65 78 74 00 00 00 DE 00 00 00 10 00 00 00 | .text I +
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 | .rdata
000001E0: 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 | p -
000001F0: 70 00 00 00 00 20 00 00 00 02 00 00 00 06 00 00 | @
00000200: 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 | .data <
00000210: 2E 64 61 74 61 00 00 00 3C 00 00 00 00 30 00 00 | .relloc
00000220: 00 02 00 00 00 08 00 00 00 00 00 00 00 00 00 00 | F @ .
00000230: 00 00 00 00 40 00 00 C0 2E 72 65 6C 6F 63 00 00 | @ B
00000240: 46 00 00 00 40 00 00 00 02 00 00 00 00 00 00 00 |
00000250: 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 |
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 |

```

# Delimitarea header-elor

00000000:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ
00000010:	08 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 C8 00 00 00	
00000040:	0E 1F BA 0E 00 04 B9 CD 21 08 01 4C CD 21 54 68	is program cannot be run in DOS mode...
00000050:	69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F	RichUA 2
00000060:	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	
00000070:	06 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00	
00000080:	11 00 DC DC 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F	
00000090:	30 B7 2E 8F 54 C1 B2 8F 55 C1 B2 8F 54 C1 B2 8F	
000000A0:	3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F	
000000B0:	52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00	
000000C0:	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00	
000000D0:	96 0B 03 52 00 00 00 00 00 00 00 00 E0 00 02 01	
000000E0:	0B 01 0A 00 00 02 00 00 00 00 00 00 06 00 00 00	
000000F0:	00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00	
00000100:	00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00	
00000110:	05 00 01 00 00 00 00 00 00 50 00 00 00 04 00 00	
00000120:	00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00	
00000130:	00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00	
00000140:	00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00	
00000150:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000160:	00 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00	
00000170:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000180:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000190:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000001A0:	00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00	
000001B0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000001C0:	2E 74 65 78 74 00 00 00 DE 00 00 00 00 10 00 00	
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	
000001F0:	70 00 00 00 00 20 00 00 00 02 00 00 00 06 00 00	
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	
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	
00000240:	46 00 00 00 40 00 00 00 00 02 00 00 00 00 00 00	
00000250:	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42	
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	

# Cuprins

- 1 Header-ele unui executabil
- 2 Image DOS Header**
- 3 Image NT Headers
- 4 Header-ele secțiunilor

# Image DOS Header

```

00000000: 4D 5A 90 00 00 00 00 00 00 00 00 00 00 00 00 00 | MZ. . . . .
00000010: 00 00 00 00 00 00 00 00 00 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 00 00 00 00 | . . . . .
00000040: 0E 1F BA 0E 00 04 00 CD 21 88 01 4C C0 21 54 68 | . . . . .
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F | is program canno
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 | mode...$
00000080: 11 A0 DC DC 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F | 4 UUUA ZUA ZUA Z
00000090: 3A B7 2E 8F 56 C1 B2 8F 55 C1 B3 8F 56 C1 B2 8F | :-ZUA ZUA ZUA Z
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F | :-ZTA Z:-ZTA Z
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 | RichUA Z
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE L.
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 00 00 02 01 | -<OR f.
000000E0: 00 01 0A 00 00 02 00 00 00 00 00 00 00 00 00 00 | . . . + -
000000F0: 00 10 00 00 00 10 00 00 20 00 00 00 00 40 00 | + + +
00000100: 00 10 00 00 00 02 00 05 00 01 00 00 00 00 00 | + + +
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 00 00 00 | . . . P .
00000120: 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 | . . . + +
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 | + + +
00000140: 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 | + + +
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
00000160: 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 | . . .
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 | . . .
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
000001C0: 2E 74 65 78 74 00 00 DE 00 00 00 00 10 00 00 | .text I +
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 | . . .
000001E0: 00 00 00 00 20 00 60 2E 72 64 61 74 61 00 00 | .rdata
000001F0: 70 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 40 | .data < 0
00000210: 2E 64 61 74 61 00 00 3C 00 00 00 00 30 00 00 | . . .
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .
00000230: 00 00 00 00 40 00 C0 2E 72 65 6C 6F 63 00 00 | . . .
00000240: 46 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 42 | . . .
00000260: 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 | . . .
00000280: 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 | . . .
000002A0: 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 | . . .
000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . .

```

# Image DOS Header

```

00000000: 40 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ.....|
00000010: 00 00 00 00 00 00 00 00 00 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 00 00 00 00 | |
00000040: 0E 1F BA 0E 00 04 09 CD 21 88 01 4C C0 21 54 68 | .5. .!..LiTh|
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F | is program canno|
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS|
00000070: 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 | mode....$|
00000080: 11 A0 DC 55 C1 82 8F 55 C1 82 8F 55 C1 82 8F | 11UUA 2UA 2UA 2|
00000090: 3A B7 2E 8F 56 C1 82 8F 55 C1 83 8F 56 C1 82 8F | :-2UA 2UA2UA 2|
000000A0: 3A B7 2C 8F 54 C1 82 8F 3A B7 2F 8F 54 C1 82 8F | :-2TA 2:-2TA 2|
000000B0: 52 69 63 68 55 C1 82 8F 00 00 00 00 00 00 00 00 | RichUA 2|
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE L..|
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 | -<OR f..|
000000E0: 00 01 0A 00 00 02 00 00 00 00 00 00 00 00 00 00 | .. + - |
000000F0: 00 10 00 00 00 10 00 00 20 00 00 00 00 00 40 00 | + + + |
00000100: 00 10 00 00 00 02 00 05 00 01 00 00 00 00 00 00 | + + + |
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 00 00 00 00 | . . P . |
00000120: 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 00 | . . . |
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 | + + + |
00000140: 00 00 00 00 00 00 10 20 00 00 28 00 00 00 00 00 | + + + |
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
00000160: 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 00 | |
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 | + |
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
000001C0: 2E 74 65 78 74 00 00 DE 00 00 00 00 10 00 00 | .text I + |
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 20 00 00 00 00 00 00 00 00 00 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 3C 00 00 00 00 30 00 00 00 | .data < 0 |
00000220: 00 02 00 00 00 00 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 | |
00000240: 46 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 | |
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 | F |
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 | |

```

```

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

```

00000000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  |MZ.....|
00000010: 00 00 00 00 00 00 00 00 00 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 00 00 00 00  |.....|
00000040: 0E 1F BA 0E 00 04 09 CD 21 08 01 4C C0 21 54 68  |.5. .it.LiTh|
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F  |is program canno|
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  |t be run in DOS|
00000070: 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00  |mode...$|
00000080: 11 A0 DC DC 55 C1 82 8F 55 C1 82 8F 55 C1 82 8F  |  UUUA ZUA ZUA Z|
00000090: 3A B7 2E 8F 56 C1 82 8F 55 C1 83 8F 56 C1 82 8F  |::ZUA ZUA ZUA Z|
000000A0: 3A B7 2C 8F 54 C1 82 8F 3A B7 2F 8F 54 C1 82 8F  |::ZTA Z::ZTA Z|
000000B0: 52 69 63 68 55 C1 82 8F 00 00 00 00 00 00 00 00  |RichUA Z|
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  |PE L.|
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 00 E0 02 01  |.BOR  f  |
000000E0: 00 01 0A 00 00 02 00 00 00 06 00 00 00 00 00 00  |. + -  |
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00  |. + +  |
00000100: 00 10 00 00 00 02 00 05 00 01 00 00 00 00 00 00  |. + + P  |
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 0A 00 00 00  |. + + P  |
00000120: 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 00  |. + +  |
00000130: 00 00 10 00 00 10 00 00 00 00 00 18 00 00 00 00  |. + +  |
00000140: 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 00  |. + (  |
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.  |
00000160: 00 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00  |.  |
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.  |
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.  |
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.  |
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00  |. +  |
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.  |
000001C0: 2E 74 65 78 74 00 00 DE 00 00 00 00 10 00 00 00  |.text I +  |
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 00 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 3C 00 00 00 00 30 00 00 00  |.data <  |
00000220: 00 02 00 00 00 00 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  |.  |
00000240: 46 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00  |F  |
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42  |.  |
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  |.  |

```

```

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

```

00000000: 40 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ |
00000010: 00 00 00 00 00 00 00 00 00 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 00 00 00 00 |  |
00000040: 0E 1F BA 0E 00 04 09 CD 21 08 01 4C C0 21 54 68 |  |
00000050: 69 73 20 70 72 6F 67 72 61 60 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 0A 24 00 00 00 00 00 00 00 00 |  |
00000080: 11 A0 DC 55 C1 82 8F 55 C1 82 8F 55 C1 82 8F |  |
00000090: 3A B7 2E 8F 56 C1 82 8F 55 C1 83 8F 56 C1 82 8F |  |
000000A0: 3A B7 2C 8F 54 C1 82 8F 3A B7 2F 8F 54 C1 82 8F |  |
000000B0: 52 69 63 68 55 C1 82 8F 00 00 00 00 00 00 00 00 |  |
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE |
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 |  |
000000E0: 00 01 0A 00 00 02 00 00 00 06 00 00 00 00 00 00 |  |
000000F0: 00 10 00 00 00 10 00 00 20 00 00 00 00 40 00 |  |
00000100: 00 10 00 00 02 00 05 00 01 00 00 00 00 00 00 |  |
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 0A 00 00 |  |
00000120: 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 |  |
00000130: 00 00 10 00 00 10 00 00 00 00 00 18 00 00 00 |  |
00000140: 00 00 00 00 00 00 10 20 00 28 00 00 00 00 00 |  |
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
00000160: 00 00 00 00 00 00 00 00 40 00 30 00 00 00 00 |  |
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 |  |
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |
000001C0: 2E 74 65 78 74 00 00 DE 00 00 00 00 10 00 00 | .text |
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 |  |
000001E0: 00 00 00 00 20 00 60 2E 72 64 61 74 61 00 00 | .rdata |
000001F0: 70 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 40 00 00 00 40 |  |
00000210: 2E 64 61 74 61 00 00 3C 00 00 00 00 30 00 00 | .data |
00000220: 00 02 00 00 00 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 |  |
00000240: 46 00 00 00 40 00 00 00 02 00 00 00 0A 00 00 |  |
00000250: 00 00 00 00 00 00 00 00 00 00 40 00 00 00 42 |  |
00000260: 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 |  |
00000280: 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 |  |
000002A0: 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 |  |
000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |  |

```

```

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

```

00000000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ. . . . .
00000010: 00 00 00 00 00 00 00 00 00 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 00 00 00 00 | . . . . .
00000040: 0E 1F BA 0E 00 04 09 CD 21 08 01 4C C0 21 54 68 | . . . . .
00000050: 69 73 20 70 72 6F 72 61 60 20 68 61 6E 6E 6F | . . . . .
00000060: 74 20 62 65 20 72 75 6E 20 69 20 44 4F 53 20 | . . . . .
00000070: 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 | . . . . .
00000080: 11 00 DC DC 55 C1 82 8F 55 C1 82 8F 55 C1 82 8F | . . . . .
00000090: 3A B7 2E 8F 56 C1 82 8F 55 C1 83 8F 56 C1 82 8F | . . . . .
000000A0: 3A B7 2C 8F 54 C1 82 8F 3A B7 2F 8F 54 C1 82 8F | . . . . .
000000B0: 52 69 63 68 55 C1 82 8F 00 00 00 00 00 00 00 00 | . . . . .
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | . . . . .
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 | . . . . .
000000E0: 00 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 | . . . . .
000000F0: 00 10 00 00 00 10 00 00 20 00 00 00 00 40 00 | . . . . .
00000100: 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 | . . . . .
00000110: 05 00 01 00 00 00 00 00 50 00 00 00 00 00 00 00 | . . . . .
00000120: 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 00 | . . . . .
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 | . . . . .
00000140: 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 00 | . . . . .
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
00000160: 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 00 | . . . . .
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . .
000001C0: 2E 74 65 78 74 00 00 DE 00 00 00 00 10 00 00 | . . . . .
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 | . . . . .
000001F0: 70 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 | . . . . .
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 3C 00 00 00 00 30 00 00 00 | . . . . .
00000220: 00 02 00 00 00 00 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 | . . . . .
00000240: 46 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 | . . . . .
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 | . . . . .
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 | . . . . .

```

```

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

- 1 Header-ele unui executabil
- 2 Image DOS Header
- 3 Image NT Headers
- 4 Header-ele secțiunilor

# Image NT Headers

```

00000000: 4D 5A 98 00 03 00 00 00 04 00 00 00 FF FF 00 00 |MZ.....|
00000010: 00 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 C8 00 00 00 |.....C....|
00000040: 0E 1F 8A 0E 00 04 09 CD 21 B8 01 4C CD 21 54 68 |.ESP...it.Li!th|
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F |is program canno|
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 |t be run in DOS|
00000070: 6D 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00 |mode...$|
00000080: 11 A0 DC 0C 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F |UUA ZUA ZUA Z|
00000090: 3A B7 2E 8F 56 C1 B2 8F 55 C1 B3 8F 56 C1 B2 8F |-.ZUA ZUA ZUA Z|
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F |-.ZTA Z-:ZTA Z|
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 |RichUA Z|
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 |PE L...|
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 |-OR...f...|
000000E0: 00 01 00 00 00 02 00 00 00 06 00 00 00 00 00 00 |...-...|
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00 |...+...+...@|
00000100: 00 10 00 00 00 02 00 00 00 05 00 01 00 00 00 00 |...+...+...+|
00000110: 05 00 01 00 00 00 00 00 00 50 00 00 00 00 04 00 |...+...+...+|
00000120: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 |...+...+...+|
00000130: 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 |...+...+...+|
00000140: 00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 |...+...+...+|
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...+...+...+|
00000160: 00 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 |...@...|
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...|
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...|
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...|
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |...+...|
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...|
000001C0: 2E 74 65 78 74 00 00 00 DE 00 00 00 10 00 00 00 |.text...+...|
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 |...rdata...|
000001E0: 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 |p...@...@|
000001F0: 70 00 00 00 20 00 00 00 00 02 00 00 00 06 00 00 |.data <...|
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 |...|
00000210: 2E 64 61 74 61 00 00 00 3C 00 00 00 30 00 00 00 |...|
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...|
00000230: 00 00 00 00 40 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...@...@ B|
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 |...@...|
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 |...|

```

```

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

```

# Image NT Headers

```

00000000: 4D 5A 98 00 03 00 00 00 04 00 00 00 FF FF 00 00 |MZ.....|
00000010: 00 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 C8 00 00 00 |.....C8....|
00000040: 0E 1F 8A 0E 00 04 09 CD 21 B8 01 4C CD 21 54 68 |.ESP..it..LitH|
00000050: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F |is program canno|
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 |t be run in DOS|
00000070: 6D 6F 64 65 2E 00 0D 0A 24 00 00 00 00 00 00 00 |mode...$.|
00000080: 11 A0 DC 0C 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F |  UUUA ZUA ZUA Z|
00000090: 3A B7 2E 8F 56 C1 B2 8F 55 C1 B3 8F 56 C1 B2 8F |--ZUA ZUA ZUA Z|
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F |--ZTA Z--ZTA Z|
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 |RichUA Z|
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 |PE L..|
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 E0 00 02 01 |.OR f..|
000000E0: 00 01 00 00 00 02 00 00 00 06 00 00 00 00 00 00 |... -|
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00 |+ + + + @|
00000100: 00 10 00 00 00 02 00 00 00 05 00 01 00 00 00 00 |+ + + +|
00000110: 05 00 01 00 00 00 00 00 00 50 00 00 00 04 00 00 |. . P + +|
00000120: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 |. @. + +|
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 |+ + + +|
00000140: 00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 |+ + + +|
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |+ + + +|
00000160: 00 00 00 00 00 00 00 00 00 40 00 00 30 00 00 00 | @ @|
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |+ + + +|
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |+ + + +|
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |+ + + +|
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |+|
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |+|
000001C0: 2E 74 65 78 74 00 00 00 DE 00 00 00 10 00 00 00 |.text | +|
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 |.rdata|
000001E0: 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 |p | @ @|
000001F0: 70 00 00 00 20 00 00 00 00 02 00 00 00 06 00 00 |.data < @|
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 |. . . .|
00000210: 2E 64 61 74 61 00 00 00 3C 00 00 00 00 30 00 00 |. . . .|
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. . . .|
00000230: 00 00 00 00 40 00 C0 2E 72 65 6C 6F 63 00 00 00 |. . . .|
00000240: 46 00 00 00 00 40 00 00 00 02 00 00 00 00 00 00 |F @ . . . .|
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 |. . . .|
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 |. . . .|

```

```

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;
};

```

00000000:	40	5A	90	00	03	00	00	00	04	00	00	FF	FF	00	00	
00000010:	B8	00	00	00	00	00	00	00	04	00	00	00	00	00	00	
00000020:	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	C8	00	00	00	
00000040:	0E	F1	BA	0E	00	04	09	CD	21	B8	01	4C	D0	21	54	68
00000050:	69	73	20	78	72	6F	67	72	61	6D	20	6B	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	20	00	00	0A	24	00	00	00	00	00	00	00
00000080:	11	A0	D0	D0	D5	C1	B2	8F	55	C1	B2	8F	55	C1	B2	8F
00000090:	38	67	2E	8F	54	C1	B2	8F	55	C1	B2	8F	55	C1	B2	8F
000000A0:	3A	67	2C	8F	54	C1	B2	8F	5A	67	2F	8F	54	C1	B2	8F
000000B0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0:	00	00	00	00	00	00	00	00	00	45	00	00	00	00	00	00
000000D0:	96	00	D3	52	00	00	00	00	00	00	00	E0	00	02	01	00
000000E0:	08	01	0A	00	00	02	00	00	00	06	00	00	00	00	00	00
000000F0:	00	10	00	00	00	10	00	00	00	20	00	00	00	00	00	00
00000100:	00	10	00	00	00	02	00	00	05	00	01	00	00	00	00	00
00000110:	05	00	01	00	00	00	00	00	00	50	00	00	00	00	00	00
00000120:	00	00	00	00	03	00	40	81	00	00	10	00	00	10	00	00
00000130:	00	00	10	00	00	10	00	00	00	00	00	10	00	00	00	00
00000140:	00	00	00	00	00	00	00	10	20	00	28	00	00	00	00	00
00000150:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160:	00	00	00	00	00	00	00	00	00	40	00	30	00	00	00	00
00000170:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180:	00	00	00	00	00	00	00	00	00	00	00	00	00	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	00	00	00	00	00	00	00	00
000001B0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0:	2E	74	65	78	7A	00	00	DE	00	00	00	10	00	00	00	00
000001D0:	00	02	00	00	00	04	00	00	00	00	00	00	00	00	00	00
000001E0:	00	00	00	00	00	20	00	60	2E	72	64	61	74	61	00	00
000001F0:	70	00	00	00	00	20	00	00	00	02	00	00	00	06	00	

```

struct _IMAGE_OPTIONAL_HEADER {
0x00 WORD Magic;
0x02 BYTE MajorLinkerVersion;
0x03 BYTE MinorLinkerVersion;
0x04 DWORD SizeOfCode;
0x08 DWORD SizeOfUninitializedData;
0x0c DWORD SizeOfInitializedData;
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];
};

```

```
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;
};
```

# Cuprins

- 1 Header-ele unui executabil
- 2 Image DOS Header
- 3 Image NT Headers
- 4 Header-ele secțiunilor**



# Image Section Headers (1)

```

00000000: 40 5A 98 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ.....
00000010: 08 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 00 C8 00 00 | .
00000040: 0E 1F BA 0E 00 04 00 CD 21 08 01 4C CD 21 54 68 | .!.!.Little
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F | is program canno
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS
00000070: 6D 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00 | mode...$
00000080: 11 A0 DC DC 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F | .UUUA ZUA ZUA Z
00000090: 3A B7 2E 8F 56 C1 B2 8F 55 C1 B3 8F 56 C1 B2 8F | .:ZUA ZUA ZUA Z
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F | .:ZUA ZUA ZUA Z
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 | RichUA Z
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE L.
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 00 E0 00 02 01 | .R
000000E0: 08 01 0A 00 00 02 00 00 00 06 00 00 00 00 00 00 | .
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00 | .
00000100: 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 | .
00000110: 05 00 01 00 00 00 00 00 00 50 00 00 00 0A 00 00 | .
00000120: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 | .
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 | .
00000140: 00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 00 | .
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .
00000160: 00 00 00 00 00 00 00 00 00 00 40 00 30 00 00 00 | .
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .
000001A0: 00 20 00 00 10 00 00 00 00 00 00 00 00 00 00 00 | .
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .
000001C0: 2E 74 65 78 74 00 00 00 DE 00 00 00 00 10 00 00 | .text I +
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 02 00 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 00 00 00 00 00 00 00 00 00 00 00 | .
00000230: 00 00 00 00 40 00 00 C9 2E 72 65 6C 6F 63 00 00 | .
00000240: 46 00 00 00 00 40 00 00 00 00 02 00 00 00 00 00 | F
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 | .
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 | .

```

```

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)

```

00000000: 40 5A 98 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ.....
00000010: 08 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 00 C8 00 00 | .
00000040: 0E 1F 0A 0E 00 04 00 CD 21 08 01 4C CD 21 54 68 | .!. Little
00000050: 69 73 20 70 72 6F 67 72 61 60 20 63 61 6E 6E 6F | is program canno
00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS
00000070: 60 6F 64 65 2E 00 00 0A 24 00 00 00 00 00 00 00 | mode...$
00000080: 11 A0 DC DC 55 C1 B2 8F 55 C1 B2 8F 55 C1 B2 8F | 4 UUUU 2U 2U 2
00000090: 3A B7 2E 8F 56 C1 B2 8F 55 C1 B3 8F 56 C1 B2 8F | :..2U 2U 2U 2
000000A0: 3A B7 2C 8F 54 C1 B2 8F 3A B7 2F 8F 54 C1 B2 8F | :..2U 2U 2U 2
000000B0: 52 69 63 68 55 C1 B2 8F 00 00 00 00 00 00 00 00 | RichU 2
000000C0: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | PE L.
000000D0: 96 AB D3 52 00 00 00 00 00 00 00 00 00 E0 02 01 | -OR
000000E0: 08 01 0A 00 00 02 00 00 00 06 00 00 00 00 00 00 | .
000000F0: 00 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00 | +
00000100: 00 10 00 00 00 02 00 00 05 01 00 00 00 00 00 00 | +
00000110: 05 00 01 00 00 00 00 00 00 50 00 00 00 0A 00 00 | |
00000120: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00 | +
00000130: 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 | +
00000140: 00 00 00 00 00 00 00 00 00 10 20 00 00 28 00 00 | +
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | +
00000160: 00 00 00 00 00 00 00 00 00 00 40 00 30 00 00 00 | a
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | a
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | +
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | +
000001A0: 00 20 00 00 00 10 00 00 00 00 00 00 00 00 00 00 | +
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | +
000001C0: 2E 74 65 78 74 00 00 00 DE 00 00 00 00 10 00 00 | .text I
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 | .rdata
000001E0: 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 | .data
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 | a
00000210: 2E 64 61 74 61 00 00 00 3C 00 00 00 00 30 00 00 | .data <
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 00 2E 72 65 65 6F 65 00 00 | a
00000240: 46 00 00 00 40 00 00 00 00 00 02 00 00 00 00 00 | R
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 | F
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 | 

```

```

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 00 00 00 10 00 00 : .text 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001E0: 00 00 00 00 20 00 00 60 12E 72 64 61 74 61 00 : p .rdata 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001F0: 70 00 00 00 00 20 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000210: 2E 64 61 74 61 00 00 00 00 00 00 30 00 00 : .data < 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000230: 00 00 00 00 40 00 00 00 12E 72 65 6C 6F 63 00 : F 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000240: 46 00 00 00 00 40 00 00 00 00 02 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 00 42 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000400: 68 04 30 40 00 68 31 30 1400 E8 C9 00 00 83 : h 0 0 0 h 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000410: C4 08 68 00 30 40 00 68 12E 30 40 00 E8 B1 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000420: 00 03 C4 00 C7 05 30 30 40 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000430: 00 30 40 00 0B D7 51 8B C3 33 D2 B9 04 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000440: F7 F1 83 FA 00 74 02 EB 121 C7 05 34 30 40 00 : . 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000450: 00 00 00 00 0B C3 33 D2 B9 05 00 00 F7 E1 83 C0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000460: 01 F7 E3 A3 34 30 40 00 EB 20 C7 05 34 30 40 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000470: 00 00 00 0B C3 33 C0 01 B8 07 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000480: 00 00 00 F7 F3 A3 34 30 1400 01 38 30 40 00 8B : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000490: 1D 34 30 40 00 03 C3 A3 38 30 40 00 59 E2 95 68 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004A0: 1C 30 40 00 68 31 30 40 00 E8 2A 00 00 83 C4 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004B0: 00 FF 35 30 30 40 00 68 12E 30 40 00 E8 17 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004C0: 00 83 C4 08 6A 00 E8 01 00 00 00 CC FF 25 08 20 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004D0: 40 00 FF 25 08 20 40 00 FF 25 04 20 40 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

```

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 00 00 00 00 00 10 00 00 : .text 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001E0: 00 00 00 00 20 00 00 00 00 00 00 00 00 61 00 00 : p .rdata 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001F0: 70 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000210: 2E 64 61 74 61 00 00 00 00 00 00 00 00 30 00 00 : .data < 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : F 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000230: 00 00 00 00 40 00 00 00 00 00 00 00 00 63 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000240: 46 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 42 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000400: 68 04 30 40 00 00 68 31 30 14 00 00 E8 C9 00 00 83 : h 00E h100 R0 a
00000410: C4 08 68 00 30 40 00 68 12E 30 40 00 E8 B1 00 00 : 0 0 0 0 h 00E R0
00000420: 00 03 C4 C7 05 00 30 30 40 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000430: 00 30 40 00 00 D7 51 8B C3 33 D2 B9 04 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000440: F7 F1 83 FA 00 74 02 EB 121 C7 05 34 30 40 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000450: 00 00 00 00 00 00 00 00 00 00 00 00 00 F7 E1 83 C0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000460: 01 F7 E3 A3 34 30 40 00 EB 20 C7 05 34 30 40 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000470: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000480: 00 00 00 00 F7 F3 A3 34 30 14 00 00 A1 38 40 00 8B : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000490: 1D 34 30 40 00 00 C3 A3 138 30 40 00 59 E2 95 68 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004A0: 1C 30 40 00 68 31 30 40 00 E8 28 00 00 00 83 C4 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004B0: 00 FF 35 30 30 40 00 68 12E 30 40 00 E8 17 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004C0: 00 83 C4 08 6A 00 E8 01 00 00 00 CC FF 25 08 20 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000004D0: 40 00 FF 25 00 20 40 00 FF 25 04 20 40 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

```

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 00 00 00 00 00 00 10 00 00 : .text 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001D0: 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001E0: 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000001F0: 70 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000210: 2E 64 61 74 61 00 00 00 00 00 00 00 00 00 30 00 00 : .data 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000220: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000230: 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000240: 46 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000002F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000003F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
00000400: 68 04 30 00 00 68 31 30 14 00 00 E8 C9 00 00 00 83 : h00E h100 R00 a
00000410: C4 08 68 00 30 40 00 68 12 E 30 40 00 E8 B1 00 00 : 00 00 h00 R00
00000420: 00 03 C4 00 C7 05 30 30 40 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000430: 00 30 40 00 00 D7 51 8B C3 33 D2 B9 04 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000440: F7 F1 83 F6 00 74 02 EB 12 C7 05 34 30 40 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000450: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000460: 01 F7 E3 A3 34 30 40 00 EB 20 C7 05 34 30 40 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000470: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000490: 1D 34 30 40 00 00 00 C3 A3 30 30 40 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004A0: 1C 30 40 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004B0: 00 FF 35 30 30 40 00 00 00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004C0: 00 83 C4 08 6A 00 E8 01 00 00 00 CC FF 25 08 20 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000004D0: 40 00 FF 25 00 20 40 00 FF 25 04 20 40 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 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;
};

```