



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



Напишите в чат, если есть проблемы!

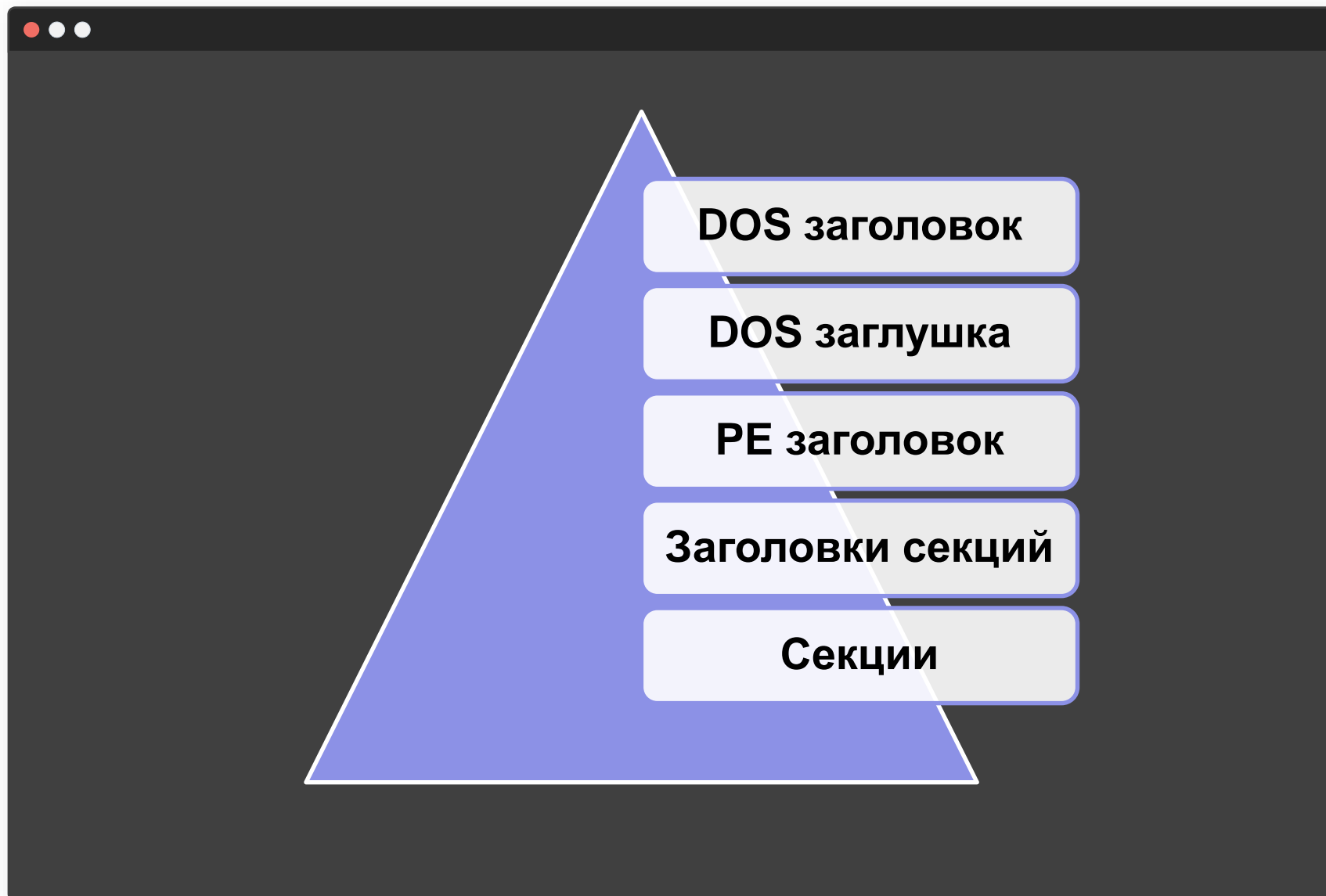
Ставьте если все хорошо

Формат исполняемых файлов **Windows**

PE формат



Структура файла

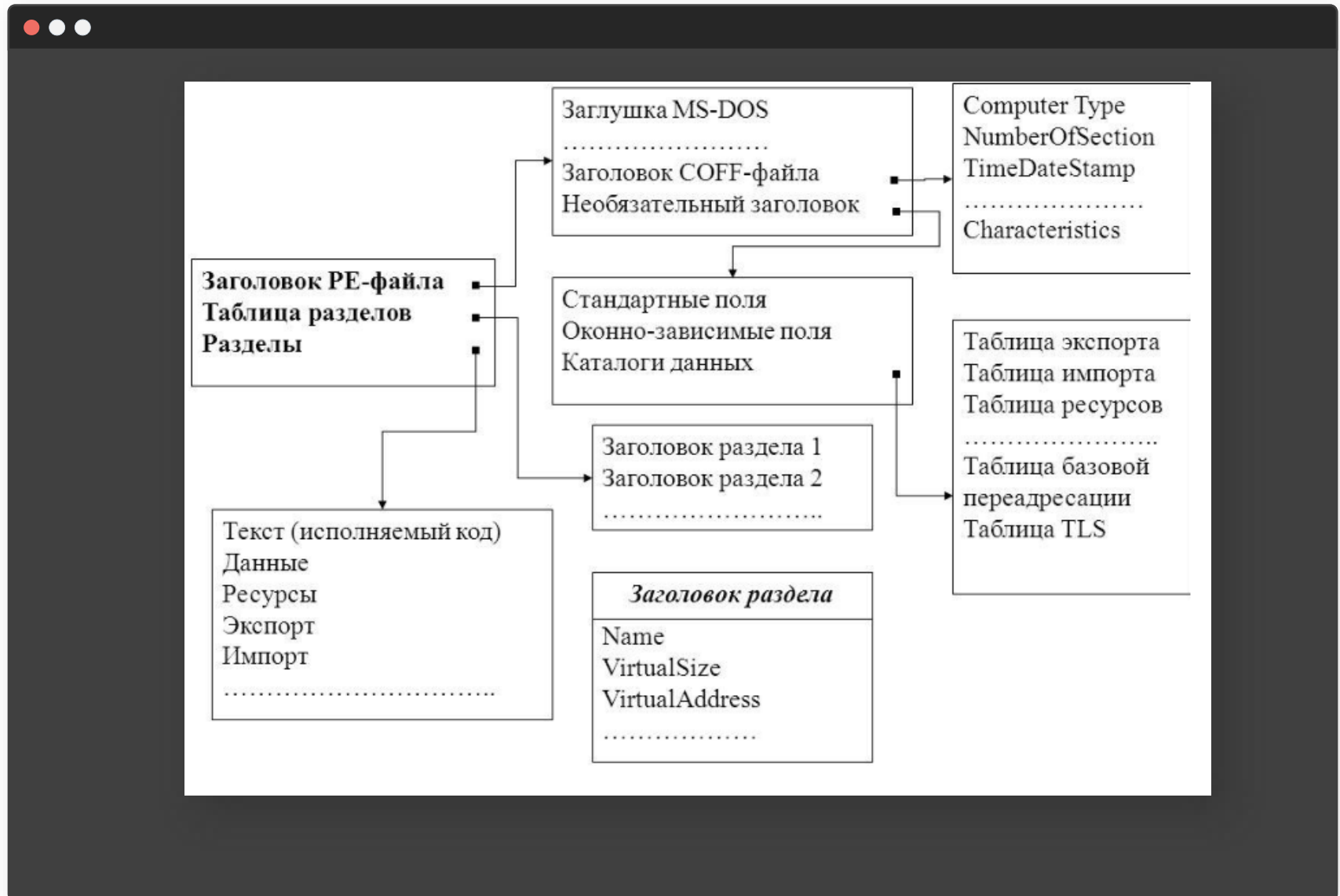


```
4D 5A 80 00-01 00 00 00-04 00 10 00-FF FF 00 00 ZA @
40 01 00 00-00 00 00 00-40 00 00 00-00 00 00 00 @
00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00 00 00 00-00 00 00 00-00 00 00 00-80 00 00 00 A

.00FE0040: 0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C-CD 21 54 68
.00FE0050: 69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F is program cannot
.00FE0060: 74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20 be run in DOS
.00FE0070: 6D 6F 64 65-2E 0D 0A 24-00 00 00 00-00 00 00 00 mode.

.00FE0080: 50 45 00 00-4C 01 02 00-0B C8 BA 5C-00 00 00 00 PE L
.00FE0090: 00 00 00 00-E0 00 0F 01-0B 01 01 47-00 02 00 00 p
.00FE00A0: 00 02 00 00-00 00 00 00-00 10 00 00-00 10 00 00
.00FE00B0: 00 20 00 00-00 00 FE 00-00 10 00 00-00 02 00 00
.00FE00C0: 01 00 00 00-00 00 00 00-03 00 0A 00-00 00 00 00
.00FE00D0: 00 30 00 00-00 02 00 00-BA ED 00 00-02 00 00 00
.00FE00E0: 00 10 00 00-00 10 00 00-00 00 01 00-00 00 00 00
.00FE00F0: 00 00 00 00-10 00 00 00-00 00 00 00-00 00 00 00
.00FE0100: 00 20 00 00-B0 00 00 00-00 00 00 00-00 00 00 00
.00FE0110: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00

00FE0160: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00FE0170: 00 00 00 00-00 00 00 00-2E 74 65 78-74 00 00 00 .text
00FE0180: 3B 00 00 00-00 10 00 00-00 02 00 00-00 02 00 00 ;
00FE0190: 00 00 00 00-00 00 00 00-00 00 00 00-20 00 00 60
00FE01A0: 2E 69 64 61-74 61 00 00-B0 00 00 00-00 20 00 00 .idata
00FE01B0: 00 02 00 00-00 04 00 00-00 00 00 00-00 00 00 00
00FE01C0: 00 00 00 00-40 00 00 C0-00 00 00 00-00 00 00 00
00FE01D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```



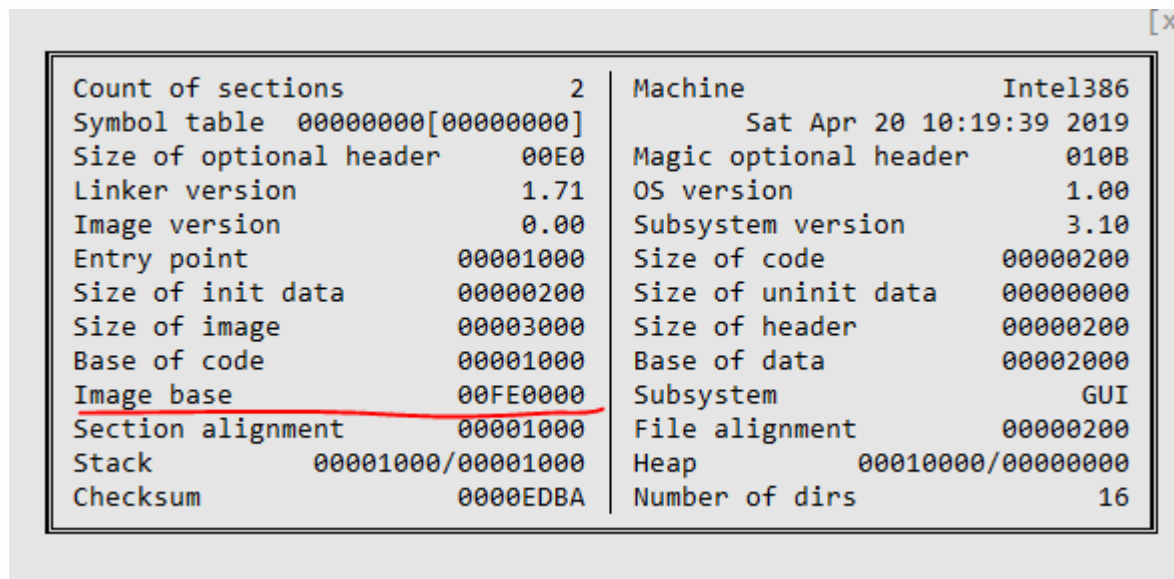
The screenshot displays the CFE Explorer VIII interface for the file HELLO_R.EXE. The left sidebar contains a tree view of file headers and various utility tools. The main pane shows a detailed property table for the file.

Property	Value
File Name	D:\Languages\iasm\EXAMPLES\HELLO\HELLO_R.EXE
File Type	Portable Executable 32
File Info	iasm -> Tomasz Grysztar
File Size	1.50 KB (1536 bytes)
PE Size	1.50 KB (1536 bytes)
Created	Tuesday 16 April 2019, 18.27.24
Modified	Saturday 20 April 2019, 10.19.39
Accessed	Tuesday 16 April 2019, 18.27.24
MD5	72599ECB3EE5DADFB6A1574B9C4640EB
SHA-1	AFB4F0D4FC7B056A8338F514F820C3675B9CBD44

Property	Value
Empty	No additional info available

https://ntcore.com/?page_id=388

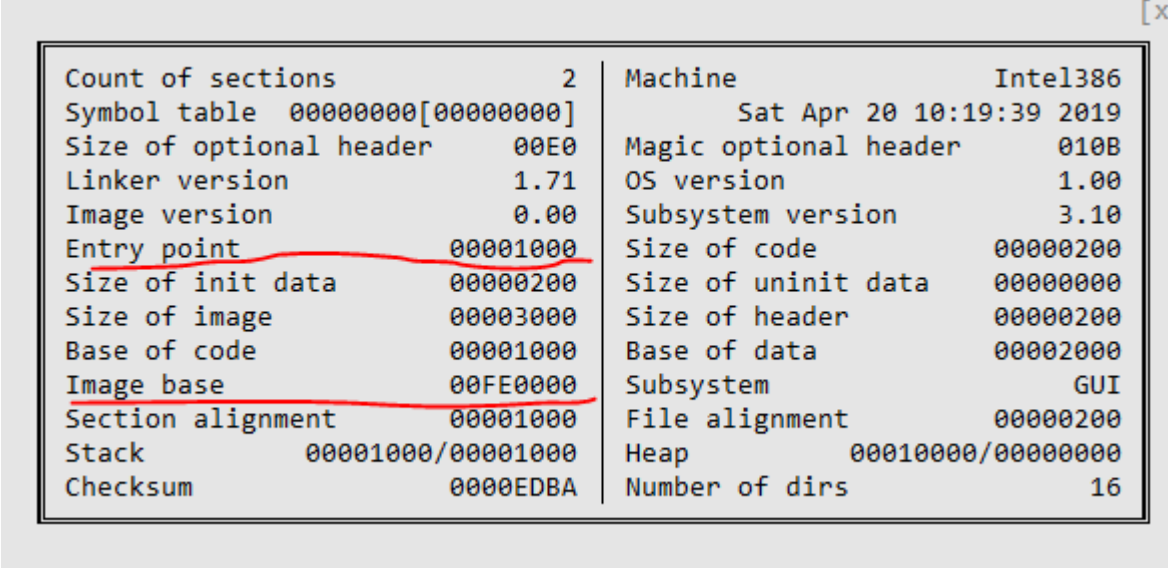
PE файлы могут быть размещены в VA процесса с 0x00000000 – 0xFFFFFFFF. Адрес размещения – базовый (imageBase)



A screenshot of a window displaying PE header information. The window has a title bar with a close button [x]. The content is a table with two columns. The 'Image base' value, 00FE0000, is underlined in red.

Count of sections	2	Machine	Intel386
Symbol table	00000000[00000000]		Sat Apr 20 10:19:39 2019
Size of optional header	00E0	Magic optional header	010B
Linker version	1.71	OS version	1.00
Image version	0.00	Subsystem version	3.10
Entry point	00001000	Size of code	00000200
Size of init data	00000200	Size of uninit data	00000000
Size of image	00003000	Size of header	00000200
Base of code	00001000	Base of data	00002000
<u>Image base</u>	<u>00FE0000</u>	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00001000/00001000	Heap	00010000/00000000
Checksum	0000EDBA	Number of dirs	16

Структура PE файла основана на относительных виртуальных адресах (**r**elative **v**irtual **a**ddress).
Считается от imageBase



Count of sections	2	Machine	Intel386
Symbol table	00000000[00000000]		Sat Apr 20 10:19:39 2019
Size of optional header	00E0	Magic optional header	010B
Linker version	1.71	OS version	1.00
Image version	0.00	Subsystem version	3.10
<u>Entry point</u>	<u>00001000</u>	Size of code	00000200
Size of init data	00000200	Size of uninit data	00000000
Size of image	00003000	Size of header	00000200
Base of code	00001000	Base of data	00002000
<u>Image base</u>	<u>00FE0000</u>	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00001000/00001000	Heap	00010000/00000000
Checksum	0000EDBA	Number of dirs	16

Любой PE файл (.exe, .dll, .sys, .cpl) начинается с DOS заголовка, описываемый структурой `_IMAGE_DOS_HEADER`

```
0:012> dt _IMAGE_DOS_HEADER
ntdll!_IMAGE_DOS_HEADER
+0x000 e_magic           : Uint2B
+0x002 e_cblp           : Uint2B
+0x004 e_cp             : Uint2B
+0x006 e_crhc          : Uint2B
+0x008 e_cpshdr        : Uint2B
+0x00a e_minalloc       : Uint2B
+0x00c e_maxalloc      : Uint2B
+0x00e e_ss            : Uint2B
+0x010 e_sp            : Uint2B
+0x012 e_csum          : Uint2B
+0x014 e_ip            : Uint2B
+0x016 e_cs            : Uint2B
+0x018 e_lfanlc        : Uint2B
+0x01a e_ovno          : Uint2B
+0x01c e_res           : [4] Uint2B
+0x024 e_oemid         : Uint2B
+0x026 e_oeminfo       : Uint2B
+0x028 e_res2          : [10] Uint2B
+0x03c e_lfanew        : Int4B
```

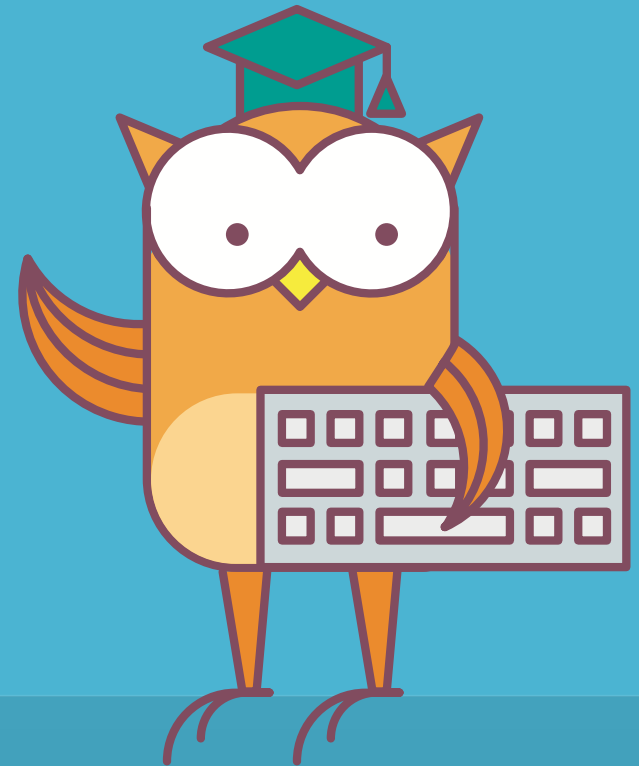

Поле `e_lfanew`, структуры `_IMAGE_DOS_HEADER` – RVA адрес до PE заголовка. Смещение этого поля = `0x3C`

```
0:012> dt _IMAGE_DOS_HEADER 00400000
ntdll!_IMAGE_DOS_HEADER
+0x000 e_magic           : 0x5a4d
+0x002 e_cblp            : 0x80
+0x004 e_cp              : 1
+0x006 e_crlc           : 0
+0x008 e_cparhdr         : 4
+0x00a e_minalloc        : 0x10
+0x00c e_maxalloc        : 0xffff
+0x00e e_ss              : 0
+0x010 e_sp              : 0x140
+0x012 e_csum            : 0
+0x014 e_ip              : 0
+0x016 e_cs              : 0
+0x018 e_lfanew         : 0x40
+0x01a e_ovno            : 0
+0x01c e_res             : [4] 0
+0x024 e_oemid           : 0
+0x026 e_oeminfo         : 0
+0x028 e_res2            : [10] 0
+0x03c e_lfanew         : 0n128
```

```
012> dt _IMAGE_DOS_HEADER 00400000
+0x03c e_lfanew         : 0n128
+0x03e e_oemid           : 0
+0x040 e_oeminfo         : 0
+0x042 e_res2            : [10] 0
+0x04c e_res             : [4] 0
```

O T U S

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

