ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

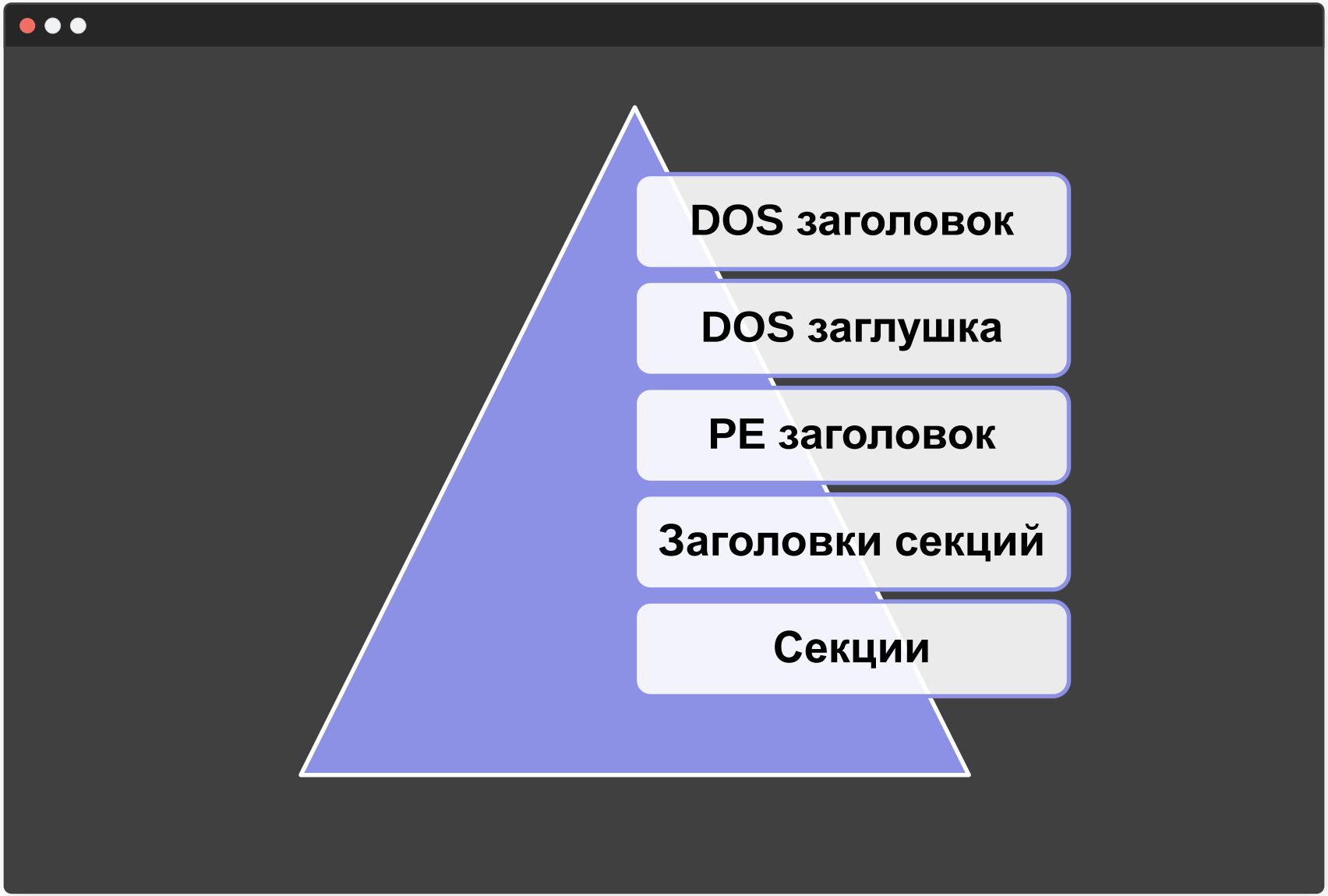
Формат исполняемых файлов **Windows**

PE формат

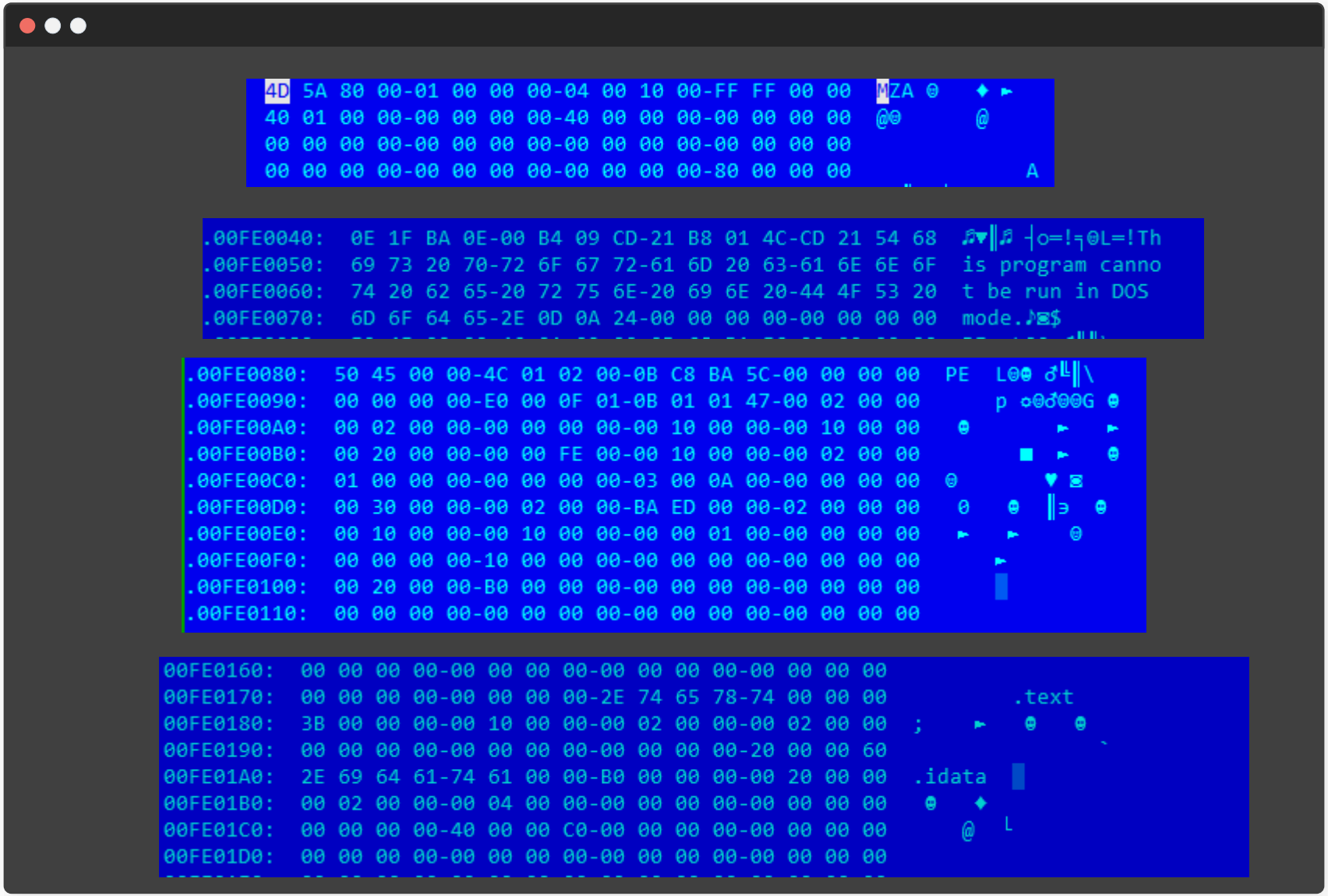
Пакулов Артур

Структура файла

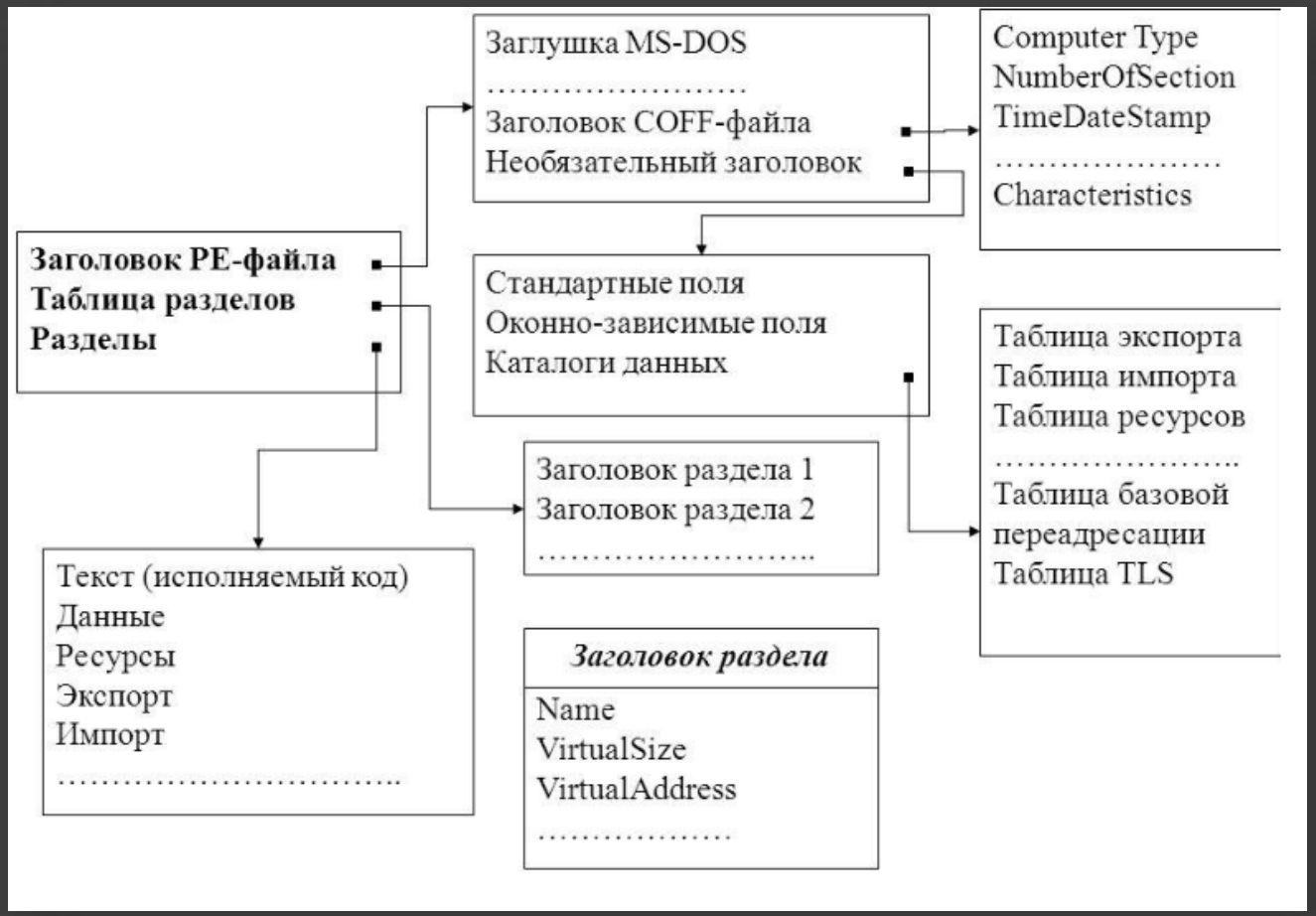
Структура файла



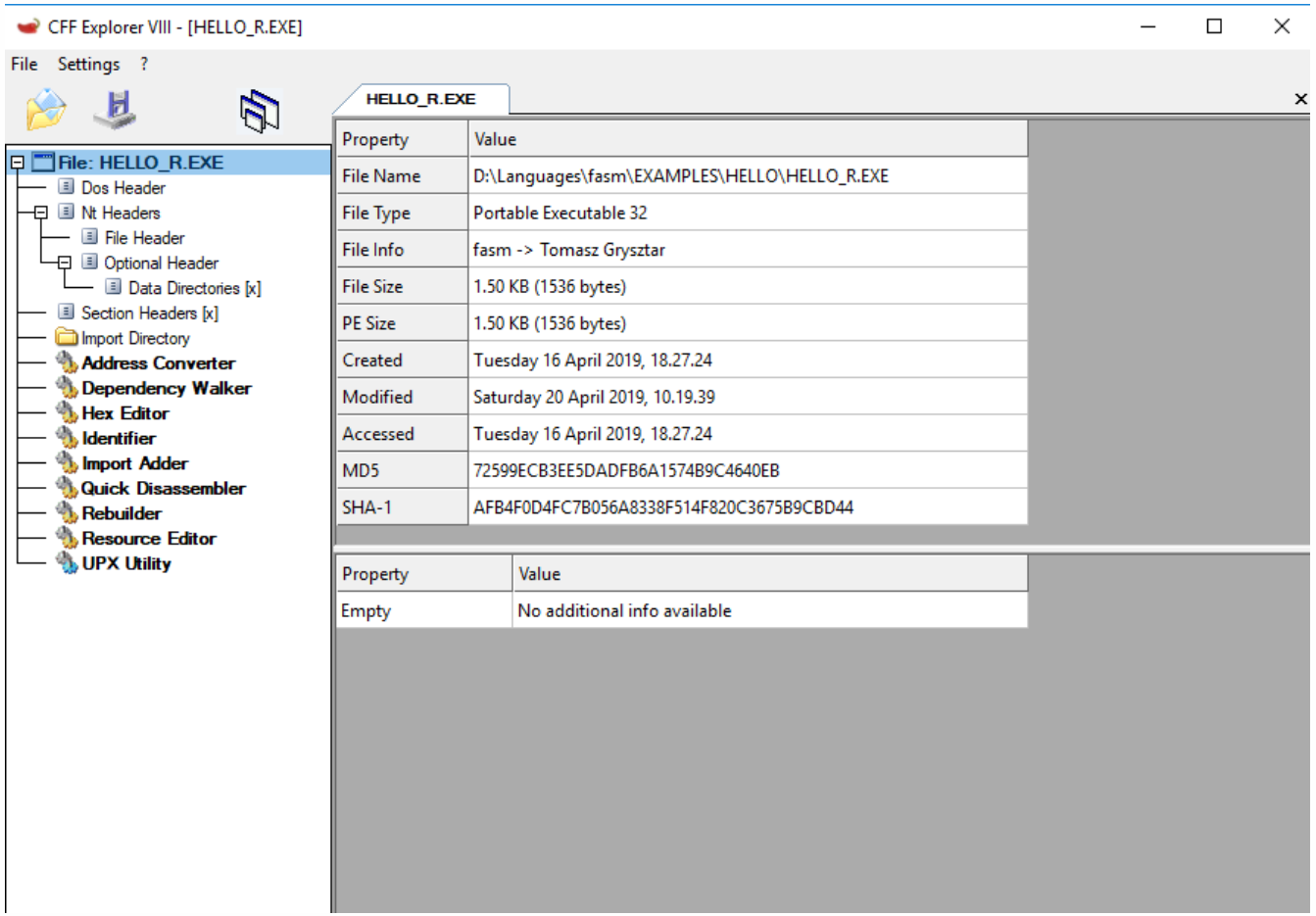
Структура файла



Структура файла



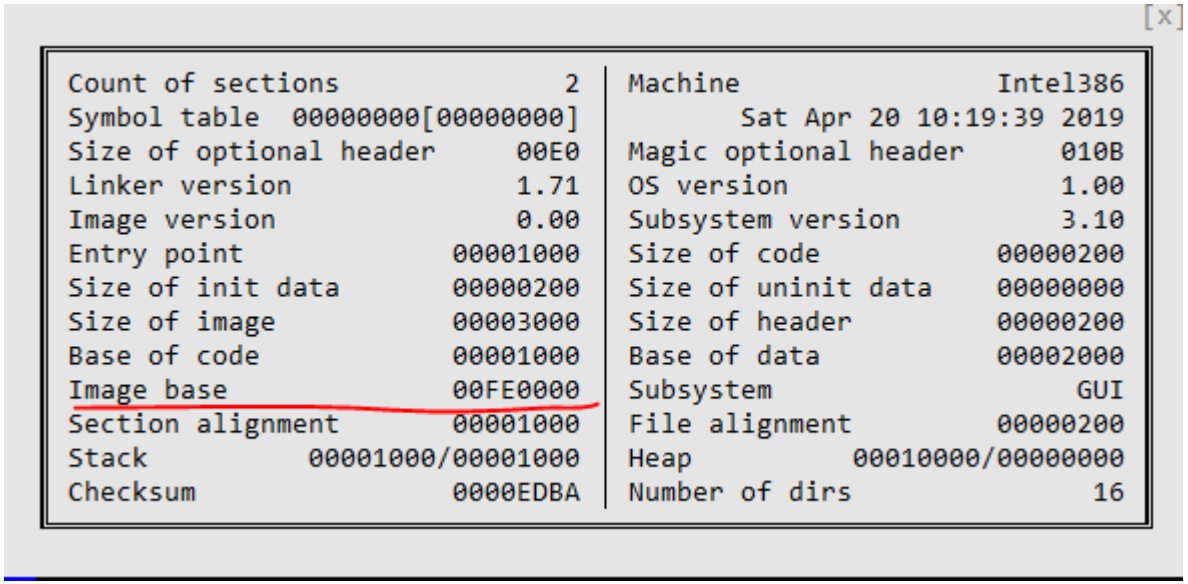
CFF explorer



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

Относительная загрузка

PE Файлы могут быть размещены в VA процесса с 0x00000000 – 0xFFFFFFFF. Адрес размещения – базовый (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
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
Image base	00FE0000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00001000/00001000	Heap	00010000/00000000
Checksum	0000EDBA	Number of dirs	16

RVA адрес

OTUS

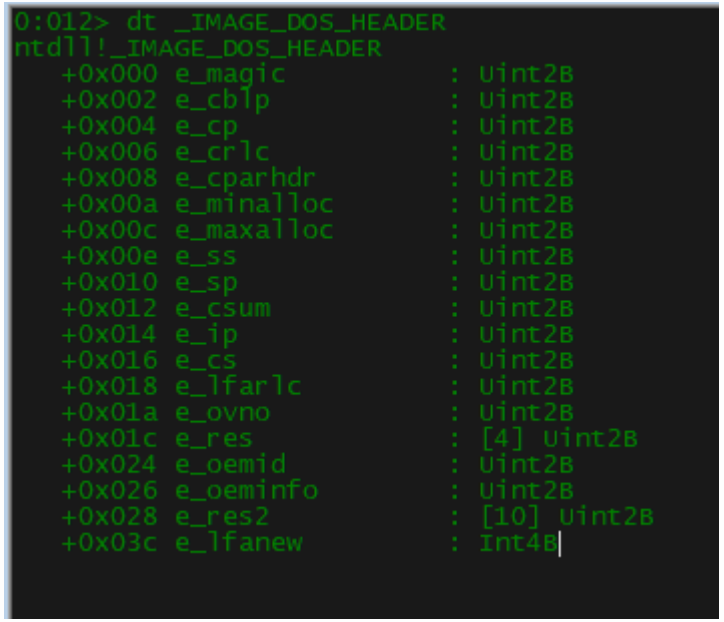
Структура PE файла основана на относительных виртуальных адресах (**r**elative **v**irtual **a**ddress). Считается от imageBase

[x]

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
Image base	00FE0000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00001000/00001000	Heap	00010000/00000000
Checksum	0000EDBA	Number of dirs	16

DOS заголовок

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



DOS заголовок

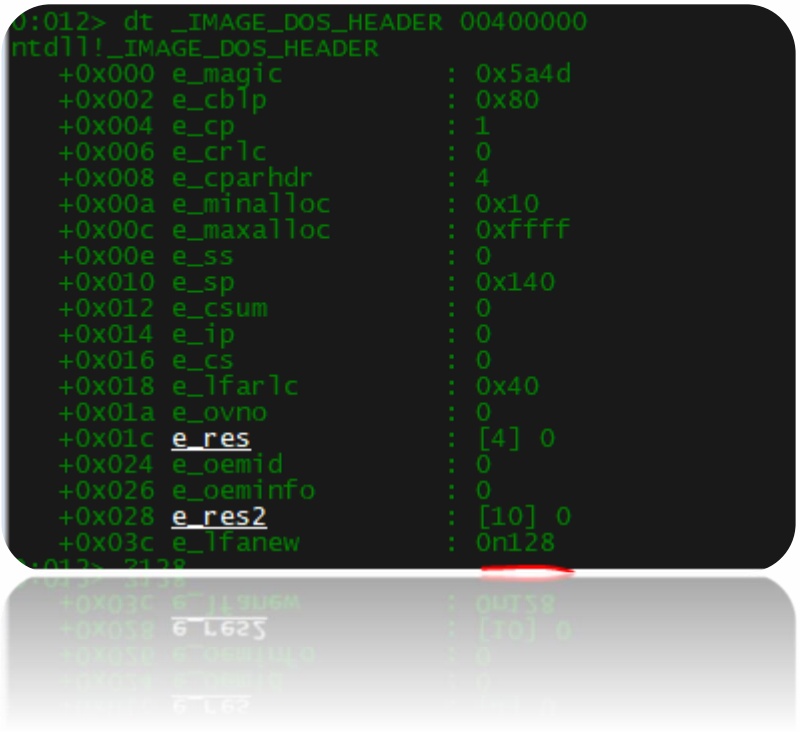
Поле e_magic, структуры _IMAGE_DOS_HEADER = 0x4d 0x5a {**MZ**}

```
0:012> dt _IMAGE_DOS_HEADER
ntdll!_IMAGE_DOS_HEADER
   +0x000 e_magic          : Uint2B
   +0x002 e_cblp           : Uint2B
   +0x004 e_cp             : Uint2B
   +0x006 e_crlc           : Uint2B
   +0x008 e_cparhdr        : 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_lfarlc         : Uint2B
   +0x01a e_ovno           : Uint2B
   +0x01c e_res            : [4] Uint2B
```

```
0:012> db 0x400000
00400000  4d 5a 80 00 01 00 00 00-04 00 10 00 ff ff 00 00  MZ..............
00400010  40 01 00 00 00 00 00 00-40 00 00 00 00 00 00 00  @.......@.......
00400020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00400030  00 00 00 00 00 00 00 00-00 00 00 00 80 00 00 00  ................
00400040  0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd 21 54 68  ........!..L.!Th
00400050  69 73 20 70 72 6f 67 72-61 6d 20 63 61 6e 6e 6f  is program canno
00400060  74 20 62 65 20 72 75 6e-20 69 6e 20 44 4f 53 20  t be run in DOS
00400070  6d 6f 64 65 2e 0d 0a 24-00 00 00 00 00 00 00 00  mode...$........
```

DOS заголовок

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



OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!