دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Youtube: onhexgroup

DOS Header

- شروع فایل **PE** با **DOS Header** هستش که بهش **MS-DOS header** هم میگن.
- در ویندوزهای مدرن خیلی کاربردی نیست و برای **MS-DOS** طراحی شده و برای سازگاری مونده.
- **MS-DOS** یا **Microsoft Disk Operating System**، اولین سیستم عاملی بود که مایکروسافت برای رایانه‌های شخصی **IBM PC** توسعه داد.

Site: onhexgroup.ir

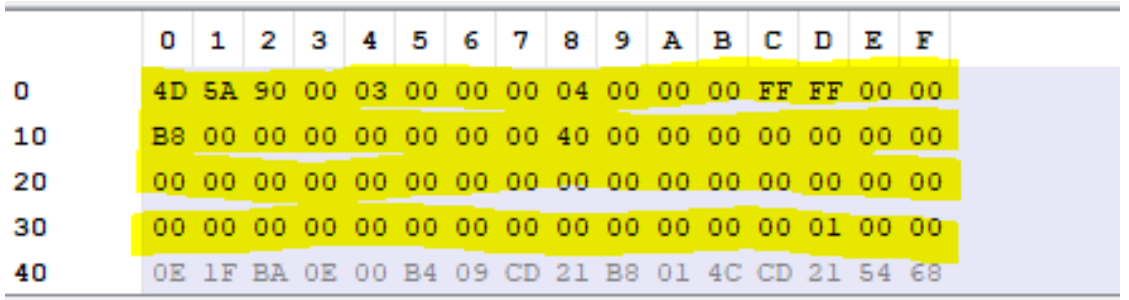
ساختار
DOS HEADER

- یک ساختار ۶۴ بایتی داره.
- ۱۹ عضو داره.
- در فایل **windows.inc** یا **winnt.h** تعریف شده.
  - C:\Program Files (x86)\Windows Kits\10\Include\[Version]\um

```
typedef struct _IMAGE_DOS_HEADER {      // DOS .EXE header
    WORD   e_magic;                     // Magic number
    WORD   e_cblp;                      // Bytes on last page of file
    WORD   e_cp;                        // Pages in file
    WORD   e_crlc;                      // Relocations
    WORD   e_cparhdr;                   // Size of header in paragraphs
    WORD   e_minalloc;                  // Minimum extra paragraphs needed
    WORD   e_maxalloc;                  // Maximum extra paragraphs needed
    WORD   e_ss;                        // Initial (relative) SS value
    WORD   e_sp;                        // Initial SP value
    WORD   e_csum;                      // Checksum
    WORD   e_ip;                        // Initial IP value
    WORD   e_cs;                        // Initial (relative) CS value
    WORD   e_lfarlc;                    // File address of relocation table
    WORD   e_ovno;                      // Overlay number
    WORD   e_res[4];                    // Reserved words
    WORD   e_oemid;                     // OEM identifier (for e_oeminfo)
    WORD   e_oeminfo;                   // OEM information; e_oemid specific
    WORD   e_res2[10];                  // Reserved words
    LONG   e_lfanew;                    // File address of new exe header
  } IMAGE_DOS_HEADER, *PIMAGE_DOS_HEADER;
```

x: onhexgroup

ساختار
DOS HEADER



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
10	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
30	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00
40	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68

Disasm | General | Strings | DOS Hdr | Rich Hdr | File Hdr | Optiona

Offset	Name	Value
0	Magic number	5A4D
2	Bytes on last page of file	90
4	Pages in file	3
6	Relocations	0
8	Size of header in paragraphs	4
A	Minimum extra paragraphs needed	0
C	Maximum extra paragraphs needed	FFFF
E	Initial (relative) SS value	0
10	Initial SP value	B8
12	Checksum	0
14	Initial IP value	0
16	Initial (relative) CS value	0
18	File address of relocation table	40
1A	Overlay number	0
1C	Reserved words[4]	0, 0, 0, 0
24	OEM identifier (for OEM information)	0
26	OEM information; OEM identifier specific	0
28	Reserved words[10]	0, 0, 0, 0, 0, 0, 0, 0, 0, 0
3C	File address of new exe header	100

Telegram: onhex_ir

فیلد
e_magic

- اولین عنصر **DOS HEADER** و سایزش **WORD**
- معروف به **Magic Number**
- یک مقدار ثابت داره: **5A4D**. معادل **MZ**
- **MZ** مخفف **Mark Zbikowsky** (یکی از طراحان اصلی **MS-DOS**)
- این فیلد مانند یک امضاء عمل میکنه و نشون دهنده اجرایی در **MS-DOS** هستش.
- در ابزارهای امنیتی مانند **YARA** قابل استفاده هستش.

Telegram: onhex_ir

فیلد
e_lfanew

- آخرین عنصر DOS HEADER و سایزش DWORD
- معروف به File address of new exe header
- مقدار آفست PE Header یا NT header یا PE signature

Site: onhexgroup.ir

ساختار PE

- مشاهده ی ساختار **PE** در:
  - **WinDBG**
  - **X64dbg**
  - **IDA Pro**