
PEfile is a library used to parse the Portable Executable format. It is very useful for malware analysis as it allows to extract informationabout the file such as Import Table, headers information and more. It also has some packer detection mechanisms with PEiD signature embedded.

```
# Output :      ----------Parsing Warnings----------

                Byte 0x00 makes up 88.7416% of the file's contents. This may indicate truncation / malformation.

                Suspicious flags set for section 2. Both IMAGE_SCN_MEM_WRITE and IMAGE_SCN_MEM_EXECUTE are set. This might indicate a packed executable.

                ----------DOS_HEADER----------

                [IMAGE_DOS_HEADER]
                0x0      0x0   e_magic:                      0x5A4D
                0x2      0x2   e_cblp:                       0x90
                0x4      0x4   e_cp:                         0x3
                0x6      0x6   e_crlc:                       0x0
                0x8      0x8   e_cparhdr:                    0x4
                0xA      0xA   e_minalloc:                   0x0
                0xC      0xC   e_maxalloc:                   0xFFFF
                0xE      0xE   e_ss:                         0x0
                0x10     0x10  e_sp:                         0xB8
                0x12     0x12  e_csum:                       0x0
                0x14     0x14  e_ip:                         0x0
                0x16     0x16  e_cs:                         0x0
                0x18     0x18  e_lfarlc:                     0x40
                0x1A     0x1A  e_ovno:                       0x0
                0x1C     0x1C  e_res:
                0x24     0x24  e_oemid:                      0x0
                0x26     0x26  e_oeminfo:                    0x0
                0x28     0x28  e_res2:
                0x3C     0x3C  e_lfanew:                     0xC8

                ----------NT_HEADERS----------

                [IMAGE_NT_HEADERS]
                0xC8     0x0   Signature:                    0x4550
```

```
----------FILE_HEADER----------


[IMAGE_FILE_HEADER]

0xCC       0x0   Machine:                       0x8664

0xCE       0x2   NumberOfSections:              0x3

0xD0       0x4   TimeDateStamp:                 0x4BC63C7D [Wed Apr 14 22:06:53 2010 UTC]

0xD4       0x8   PointerToSymbolTable:          0x0

0xD8       0xC   NumberOfSymbols:               0x0

0xDC       0x10  SizeOfOptionalHeader:          0xF0

0xDE       0x12  Characteristics:               0x23

Flags: IMAGE_FILE_EXECUTABLE_IMAGE, IMAGE_FILE_LARGE_ADDRESS_AWARE, IMAGE_FILE_RELOCS_STRIPPED


----------OPTIONAL_HEADER----------


[IMAGE_OPTIONAL_HEADER64]

0xE0       0x0   Magic:                         0x20B

0xE2       0x2   MajorLinkerVersion:            0x1

0xE3       0x3   MinorLinkerVersion:            0x0

0xE4       0x4   SizeOfCode:                    0x3000

0xE8       0x8   SizeOfInitializedData:         0x1000

0xEC       0xC   SizeOfUninitializedData:       0x0

0xF0       0x10  AddressOfEntryPoint:           0x4000

0xF4       0x14  BaseOfCode:                    0x1000

0xF8       0x18  ImageBase:                     0x140000000

0x100      0x20  SectionAlignment:              0x1000

0x104      0x24  FileAlignment:                 0x200

0x108      0x28  MajorOperatingSystemVersion:   0x4

0x10A      0x2A  MinorOperatingSystemVersion:   0x0

0x10C      0x2C  MajorImageVersion:             0x0

0x10E      0x2E  MinorImageVersion:             0x0

0x110      0x30  MajorSubsystemVersion:         0x4

0x112      0x32  MinorSubsystemVersion:         0x0

0x114      0x34  Reserved1:                     0x0

0x118      0x38  SizeOfImage:                   0x4248

0x11C      0x3C  SizeOfHeaders:                 0x248

0x120      0x40  CheckSum:                      0xA0B8

0x124      0x44  Subsystem:                     0x2
```

```
0x126      0x46  DllCharacteristics:            0x8000
0x128      0x48  SizeOfStackReserve:            0x100000
0x130      0x50  SizeOfStackCommit:             0x1000
0x138      0x58  SizeOfHeapReserve:             0x100000
0x140      0x60  SizeOfHeapCommit:              0x1000
0x148      0x68  LoaderFlags:                   0x0
0x14C      0x6C  NumberOfRvaAndSizes:           0x10
DllCharacteristics: IMAGE_DLLCHARACTERISTICS_TERMINAL_SERVER_AWARE

----------PE Sections----------

[IMAGE_SECTION_HEADER]
0x1D0      0x0   Name:                          .text
0x1D8      0x8   Misc:                          0x104E
0x1D8      0x8   Misc_PhysicalAddress:          0x104E
0x1D8      0x8   Misc_VirtualSize:              0x104E
0x1DC      0xC   VirtualAddress:                0x1000
0x1E0      0x10  SizeOfRawData:                 0x1200
0x1E4      0x14  PointerToRawData:              0x400
0x1E8      0x18  PointerToRelocations:          0x0
0x1EC      0x1C  PointerToLinenumbers:          0x0
0x1F0      0x20  NumberOfRelocations:           0x0
0x1F2      0x22  NumberOfLinenumbers:           0x0
0x1F4      0x24  Characteristics:               0x60000020
Flags: IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
Entropy: 0.168100 (Min=0.0, Max=8.0)
MD5     hash: a4a5deae25708a9e05f50bcad7075c86
SHA-1   hash: e66374a7f405687da2de82ab3fbcad13858fa6b2
SHA-256 hash: 04bf20abd166f5ae804746ecaaef3a31eca367efd50703d95f74efecb7edcd49
SHA-512 hash: 0dac9777168dd78df5610a86835102b6448b3500ec73af3036dfcf4c97860cafd46574f37f00f6548fdb3fc2b9658eafa5c7598f8ad4863889a48353c3647

[IMAGE_SECTION_HEADER]
0x1F8      0x0   Name:                          .rdata
0x200      0x8   Misc:                          0x84
0x200      0x8   Misc_PhysicalAddress:          0x84
0x200      0x8   Misc_VirtualSize:              0x84
0x204      0xC   VirtualAddress:                0x3000
0x208      0x10  SizeOfRawData:                 0x200
```

```
0x20C      0x14  PointerToRawData:              0x1600
0x210      0x18  PointerToRelocations:          0x0
0x214      0x1C  PointerToLinenumbers:          0x0
0x218      0x20  NumberOfRelocations:           0x0
0x21A      0x22  NumberOfLinenumbers:           0x0
0x21C      0x24  Characteristics:               0x40000040
Flags: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
Entropy: 0.963087 (Min=0.0, Max=8.0)
MD5     hash: 4401b01ed5cab6e12da0b4d759abb811
SHA-1   hash: eaa0ea1391a9acb394adc341e7ccde20ebabe63d
SHA-256 hash: 044a2ed87d2236d5ec62e65a1d9e53ab4d953e30fdaa883268b7534541e557f6
SHA-512 hash: e77379eec14488b1db1d46b547e76ec8f5c3365175b4d298ffeaf3892e146b07a80cca4d7271da7c98c54e80eb96184c1309c9018008a73e4fa69a25e

[IMAGE_SECTION_HEADER]
0x220      0x0   Name:                          .admx
0x228      0x8   Misc:                          0x248
0x228      0x8   Misc_PhysicalAddress:          0x248
0x228      0x8   Misc_VirtualSize:              0x248
0x22C      0xC   VirtualAddress:                0x4000
0x230      0x10  SizeOfRawData:                 0x400
0x234      0x14  PointerToRawData:              0x1800
0x238      0x18  PointerToRelocations:          0x0
0x23C      0x1C  PointerToLinenumbers:          0x0
0x240      0x20  NumberOfRelocations:           0x0
0x242      0x22  NumberOfLinenumbers:           0x0
0x244      0x24  Characteristics:               0xE0000020
Flags: IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
Entropy: 4.046846 (Min=0.0, Max=8.0)
MD5     hash: 08b807c33b87733c6f7640579169f388
SHA-1   hash: 50787b30ddcb6f50419216ccb2671c47e6a6b770
SHA-256 hash: 5f240f8e2b47a622940bd356c52ac432d4d6def62572ecde2a76c963fb122ab6
SHA-512 hash: c2d5c2d876cdfe8c28f73e6b936eb9e00f7d507c8d77d1756ea0d6c3a49aa004dff23d372e6c825b0dbddff00239664053eebb41d23a6d1986c942061f

----------Directories----------

[IMAGE_DIRECTORY_ENTRY_EXPORT]
0x150      0x0   VirtualAddress:                0x0
0x154      0x4   Size:                          0x0
```

```
[IMAGE_DIRECTORY_ENTRY_IMPORT]
0x158     0x0   VirtualAddress:            0x41D0
0x15C     0x4   Size:                      0x6C
[IMAGE_DIRECTORY_ENTRY_RESOURCE]
0x160     0x0   VirtualAddress:            0x0
0x164     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_EXCEPTION]
0x168     0x0   VirtualAddress:            0x0
0x16C     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_SECURITY]
0x170     0x0   VirtualAddress:            0x0
0x174     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_BASERELOC]
0x178     0x0   VirtualAddress:            0x4240
0x17C     0x4   Size:                      0x8
[IMAGE_DIRECTORY_ENTRY_DEBUG]
0x180     0x0   VirtualAddress:            0x0
0x184     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_COPYRIGHT]
0x188     0x0   VirtualAddress:            0x0
0x18C     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_GLOBALPTR]
0x190     0x0   VirtualAddress:            0x0
0x194     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_TLS]
0x198     0x0   VirtualAddress:            0x0
0x19C     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG]
0x1A0     0x0   VirtualAddress:            0x0
0x1A4     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT]
0x1A8     0x0   VirtualAddress:            0x0
0x1AC     0x4   Size:                      0x0
[IMAGE_DIRECTORY_ENTRY_IAT]
0x1B0     0x0   VirtualAddress:            0x3000
0x1B4     0x4   Size:                      0x18
[IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT]
0x1B8     0x0   VirtualAddress:            0x0
```

```
0x1BC      0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR]
0x1C0      0x0   VirtualAddress:              0x0
0x1C4      0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_RESERVED]
0x1C8      0x0   VirtualAddress:              0x0
0x1CC      0x4   Size:                        0x0

----------Imported symbols----------

[IMAGE_IMPORT_DESCRIPTOR]
0x19D0     0x0   OriginalFirstThunk:          0x41F8
0x19D0     0x0   Characteristics:             0x41F8
0x19D4     0x4   TimeDateStamp:               0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x19D8     0x8   ForwarderChain:              0xFFFFFFFF
0x19DC     0xC   Name:                        0x4210
0x19E0     0x10  FirstThunk:                  0x3000

KERNEL32.dll.VirtualAlloc Hint[1112]
KERNEL32.dll.ExitProcess Hint[261]

----------Base relocations----------

[IMAGE_BASE_RELOCATION]
0x1A40     0x0   VirtualAddress:              0x0
0x1A44     0x4   SizeOfBlock:                 0x8
```