

the PE Format  
Standard File & Memory layouts

offset PointerToRawData  
PSize SizeOfRawData  
address VirtualAddress  
VSize VirtualSize

offset 0

```

IMAGE_DOS_HEADER
0x00 dw e_magic MZ
0x02 dw e_cblp
0x04 dw e_cp exe size
0x06 dw e_crlc
0x08 dw e_cparhdr exe start
0x0a dw e_minalloc
0x0c dw e_maxalloc
0x0e dw e_ss
0x10 dw e_sp
0x12 dw e_csum
0x14 dw e_ip
0x16 dw e_cs
0x18 dw e_lfarlc
0x1a dw e_ovno
0x1c dw e_res[4]
0x24 dw e_oemid
0x26 dw e_oeminfo
0x28 dw e_res2[10]
0x3c dd e_lfanew

```

```

0x00 dd Signature PE,0,0 IMAGE_NT_HEADERS[32/64]
0x04 FileHeader

```

```

IMAGE_FILE_HEADER
0x00 dw Machine 0x014c/0x8664 [64b]
0x02 dw NumberOfSections
0x04 dd TimeDateStamp
0x08 dd PointerToSymbolTable
0x0c dd NumberOfSymbols
0x10 dw SizeOfOptionalHeader
0x12 dw Characteristics exe/dll, relocs

```

0x18 optionalHeader

```

IMAGE_OPTIONAL_HEADER[32/64]
0x00 dw Magic 0x10b/0x20b [64b]
0x02 db MajorLinkerVersion
0x03 db MinorLinkerVersion
0x04 dd SizeOfCode
0x08 dd SizeOfInitializedData
0x0c dd SizeOfUninitializedData
0x10 dd AddressOfEntryPoint
0x14 dd BaseOfCode
0x18 dd BaseOfData 32b only
0x1c dd ImageBase dq [64b]
0x20 dd SectionAlignment 2^y, y >=x
0x24 dd FileAlignment 2^x
0x28 dw MajorOperatingSystemVersion =4
0x2a dw MinorOperatingSystemVersion
0x2c dw MajorImageVersion
0x2e dw MinorImageVersion
0x30 dw MajorSubsystemVersion
0x32 dw MinorSubsystemVersion
0x34 dd Win32VersionValue
0x38 dd SizeOfImage
0x3c dd SizeOfHeaders
0x40 dd CheckSum drivers only
0x44 dw Subsystem driver/gui/cli
0x46 dw DllCharacteristics
0x48 dd SizeOfStackReserve dq [64b]
0x4c dd SizeOfStackCommit dq [64b]
0x50 dd SizeOfHeapReserve dq [64b]
0x54 dd SizeOfHeapCommit dq [64b]
0x58 dd LoaderFlags
0x5c dd NumberOfRvaAndSizes <=16
0x60 DataDirectory

```

SizeOfOptionalHeader

```

IMAGE_DATA_DIRECTORY
0x00 dd VirtualAddress
0x04 dd Size

```

NumberOfRvaAndSizes

Data Directories

### the PE Format (1/2) the PE Headers

relative offset →  
offset →  
RVA →

**Critical**  
standard  
minor/ignored

list  
:  
:

```

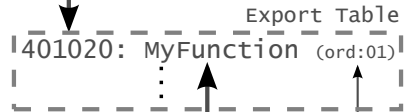
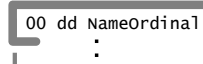
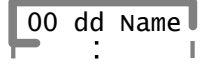
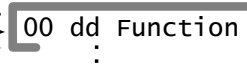
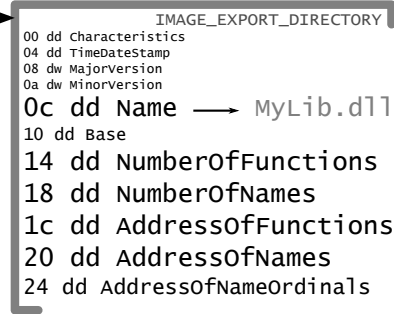
IMAGE_SECTION_HEADER
0x00 db Name[8]
0x08 dd PhysicalAddress | VirtualSize
0x0c dd VirtualAddress
0x10 dd SizeOfRawData
0x14 dd PointerToRawData
0x18 dd PointerToRelocations
0x1c dd PointerToLinenumbers
0x20 dw NumberOfRelocations
0x22 dw NumberOfLinenumbers
0x24 dd Characteristics RWX

```

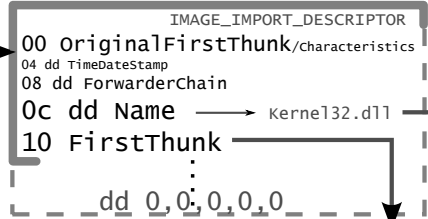
NumberOfSections

Section Table

- DATA DIRECTORIES
- 1 IMAGE\_DIRECTORY\_ENTRY\_EXPORT
  - 2 IMAGE\_DIRECTORY\_ENTRY\_IMPORT
  - 3 IMAGE\_DIRECTORY\_ENTRY\_RESOURCE
  - 4 IMAGE\_DIRECTORY\_ENTRY\_SECURITY
  - 5 IMAGE\_DIRECTORY\_ENTRY\_EXCEPTION
  - 6 IMAGE\_DIRECTORY\_ENTRY\_BASERELOC
  - 7 IMAGE\_DIRECTORY\_ENTRY\_DEBUG
  - 8 IMAGE\_DIRECTORY\_ENTRY\_COPYRIGHT
  - 9 IMAGE\_DIRECTORY\_ENTRY\_GLOBALPTR
  - A IMAGE\_DIRECTORY\_ENTRY\_TLS
  - B IMAGE\_DIRECTORY\_ENTRY\_LOAD\_CONFIG
  - C IMAGE\_DIRECTORY\_ENTRY\_BOUND\_IMPORT
  - D IMAGE\_DIRECTORY\_ENTRY\_IAT
  - E IMAGE\_DIRECTORY\_ENTRY\_DELAY\_IMPORT
  - F IMAGE\_DIRECTORY\_ENTRY\_COM\_DESCRIPTOR



the PE Format  
Data Directories 1/2



(after loading)



(on file)

