PE¹⁰² a Windows executable format overview

Portable Executable

Ange Albertini
Corkami
2009-2013

DOS Header
OFFSET 0

IMAGE_DOS_HEADER
- 00+2 e_magic MZ
- 02+2 e_cblp
- 04+2 e_cp   exe size
- 06+2 e_crlc
- 08+2 e_cparhdr   exe start
- 0a+2 e_minalloc
- 0c+2 e_maxalloc
- 0e+2 e_ss   initial ss
- 10+2 e_sp   initial sp
- 12+2 e_csum
- 14+2 e_ip
- 16+2 e_cs
- 18+2 e_lfarlc
- 1a+2 e_ovno
- 1c+8 e_res[4]
- 24+2 e_oemid
- 26+2 e_oeminfo
- 28+2 e_res2[10]
- 3c+4 **e_lfanew**

PE Header

IMAGE_NT_HEADERS(32/64)
- 00+04 Signature PE\0\0
- 04+14 FileHeader

IMAGE_FILE_HEADER
- 00+2 Machine   CPU architecture
- 02+2 NumberOfSections
- 04+4 TimeDateStamp
- 08+4 PointerToSymbolTable
- 0c+4 NumberOfSymbols
- 10+2 SizeOfOptionalHeader
- 12+2 Characteristics   exe/dll_relocs

18+60/+70 OptionalHeader

IMAGE_OPTIONAL_HEADER(32/64)
- 64b 32b
- 00+2 Magic 32b or 64b
- 02+1 MajorLinkerVersion   required with alignment
- 03+1 MinorLinkerVersion
- 04+4 04+4 SizeOfCode
- 08+4 08+4 SizeOfInitializedData
- 0c+4 0c+4 SizeOfUninitializedData
- 10+4 10+4 AddressOfEntryPoint   where execution starts
- 14+4 14+4 BaseOfCode
- ---- 18+4 BaseOfData
- 18+8 1c+4 ImageBase   suggested address to load the file
- 20+4 20+4 SectionAlignment   >=FA, with git
- 24+4 24+4 FileAlignment   =FA
- 28+2 28+2 MajorOperatingSystemVersion
- 2a+2 2a+2 MinorOperatingSystemVersion
- 2c+2 2c+2 MajorImageVersion
- 2e+2 2e+2 MinorImageVersion
- 30+2 30+2 MajorSubsystemVersion   4.0API 5.1WinNT 6.2Win10
- 32+2 32+2 MinorSubsystemVersion
- 34+4 34+4 Win32VersionValue   overwrites OS value in Thread Environment Block
- 38+4 38+4 SizeOfImage
- 3c+4 3c+4 SizeOfHeaders   not always sizeof(headers)
- 40+4 40+4 CheckSum   only used for drivers
- 44+2 44+2 Subsystem   executable driver...
- 46+2 46+2 DllCharacteristics
- 48+8 48+4 SizeOfStackReserve
- 50+8 4c+4 SizeOfStackCommit
- 58+8 50+4 SizeOfHeapReserve
- 60+8 54+4 SizeOfHeapCommit
- 68+4 58+4 LoaderFlags
- 6c+4 5c+4 NumberOfRvaAndSizes
- 70+8 60+8 VirtualAddress, Size

IMAGE_DATA_DIRECTORY[]
- 0 EXPORT
- 1 IMPORT
- 2 RESOURCE   icons, manifest, version...
- 3 EXCEPTION 64bits exceptions
- 4 SECURITY   Authenticode signatures
- 5 BASERELOC relocations
- 6 DEBUG   symbols
- 7 COPYRIGHT/Architecture   useless
- 8 GLOBALPTR only on Itanium systems
- 9 TLS   Thread Local Storage
- a LOAD_CONFIG SafeSEH
- b BOUND_IMPORT speeds up imports loading
- c IAT   Import Address Table
- d DELAY_IMPORT
- e COM_DESCRIPTOR .NET header
- f reserved   unused
(ignored)

Section Table

IMAGE_SECTION_HEADER
- 00+8 Name[8]
- 08+4 VirtualSize
- 0c+4 VirtualAddress   section start in memory
- 10+4 SizeOfRawData
- 14+4 PointerToRawData   section start in file
- 18+4 PointerToRelocations
- 1c+4 PointerToLinenumbers
- 20+2 NumberOfRelocations
- 22+2 NumberOfLinenumbers
- 24+4 Characteristics

1 Imports

IMAGE_IMPORT_DESCRIPTOR
- 00+4 OriginalFirstThunk /Characteristics
- 04+4 TimeDateStamp
- 08+4 ForwarderChain
- 0c+4 Name   Kernel32.dll
- 10+4 FirstThunk

IMAGE_THUNK_DATA(32/64)
- +8 +4 AddressOfData   /Ordinal/ForwarderString/Function

IMAGE_THUNK_DATA(32/64)
- +8 +4 AddressOfData   /Ordinal/ForwarderString/Function

IMAGE_IMPORT_BY_NAME
- 00+2 Hint
- 02+1 Name[*]

IAT
- <address> <library> <api> <hint>

0 Exports

IMAGE_EXPORT_DIRECTORY
- 00+4 Characteristics
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+4 Name   .(dll)
- 10+4 Base
- 14+4 NumberOfFunctions
- 18+4 NumberOfNames
- 1c+4 AddressOfFunctions
- 20+4 AddressOfNames
- 24+4 AddressOfNameOrdinals

"Export Table"
- 00+4 Function
- 00+4 Name
- 00+2 NameOrdinal
- <address>: <api> <ordinal>

2 Resources
(Data Directory)

ROOT
IMAGE_RESOURCE_DIRECTORY
- 00+4 Characteristics
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+2 NumberOfNamedEntries
- 0e+2 NumberOfIdEntries

IMAGE_RESOURCE_DIRECTORY_ENTRY
- 00+4 Name/ID type (RT_*)
- 04+4 OffsetToData

type
IMAGE_RESOURCE_DIRECTORY
- 00+4 Characteristics
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+2 NumberOfNamedEntries
- 0e+2 NumberOfIdEntries

IMAGE_RESOURCE_DIRECTORY_ENTRY
- 00+4 Name/ID Name/ID
- 04+4 OffsetToData

name/IDs
IMAGE_RESOURCE_DIRECTORY
- 00+4 Characteristics
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+2 NumberOfNamedEntries
- 0e+2 NumberOfIdEntries

IMAGE_RESOURCE_DIRECTORY_ENTRY
- 00+4 Name/ID language
- 04+4 OffsetToData

language
IMAGE_RESOURCE_DATA_ENTRY
- 00+4 OffsetToData
- 04+4 Size
- 08+4 CodePage
- 0c+4 Reserved

4 Exceptions

RUNTIME_FUNCTION
- 00+4 FunctionStart
- 04+4 FunctionEnd
- 08+4 UnwindInfo

UNWIND_INFO
- 00+1 Version/Flags :3 :5
- 01+1 SizeOfProlog
- 02+1 CountOfCodes
- 03+1 FrameRegister/Offset :4 :4

UNWIND_CODE
- 00+1 CodeOffset
- 01+1 UnwindOp/OpInfo :4 :4
- 02+2 FrameOffset

- ??+4 ExceptionHandler/FunctionEntry
- +4 ExceptionData[]

3 Signature

WIN_CERTIFICATE
- 00+4 dwLength
- 04+2 wRevision
- 06+2 wCertificateType
- 08+? bCertificate []

5 Relocations

IMAGE_BASE_RELOCATION
- 00+4 VirtualAddress
- 04+4 SizeOfBlock
- +2 TypeOffset   Type:4 Offset:12

relocation block
- PUSH EBP
- PUSH offset szMyString

6 Debug symbols

IMAGE_DEBUG_DIRECTORY
- 00+4 Characteristics
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+4 Type   1 Coff/2 CV-PDB/9 Borland
- 10+4 SizeOfData
- 14+4 AddressOfRawData
- 18+4 PointerToRawData

7 Copyright
<copyright string>

9 Thread Local Storage

IMAGE_TLS_DIRECTORY(32/64)
- 64b 32b
- 00+8 00+4 StartAddressOfRawData
- 08+8 04+4 EndAddressOfRawData
- 10+8 08+4 AddressOfIndex   pointer to tls index
- 18+8 0c+4 AddressOfCallBacks
- 20+4 10+4 SizeOfZeroFill
- 24+4 14+4 Characteristics
- +8 +4 Callback

A SafeSEH

IMAGE_LOAD_CONFIG_DIRECTORY(32/64)
- 00+4 Size
- 04+4 TimeDateStamp
- 08+2 MajorVersion
- 0a+2 MinorVersion
- 0c+4 GlobalFlagsClear
- 10+4 GlobalFlagsSet
- 14+4 CriticalSectionDefaultTimeout
- 18+8 18+4 DeCommitFreeBlockThreshold
- 20+8 1c+4 DeCommitTotalFreeThreshold
- 28+8 20+4 LockPrefixTable
- 30+8 24+4 MaximumAllocationSize
- 38+8 28+4 VirtualMemoryThreshold
- 40+8 2c+4 ProcessAffinityMask
- 48+4 30+4 ProcessHeapFlags
- 4c+2 34+2 CSDVersion
- 50+2 36+2 Reserved1
- 58+8 3c+4 SecurityCookie
- 60+8 40+4 SEHandlerTable
- 68+8 44+4 SEHandlerCount
- 64b 32b

HandlerTable
- 00+4 Handler

B Bound imports

IMAGE_BOUND_IMPORT_DESCRIPTOR
- 00+4 TimeDateStamp
- 04+2 OffsetModuleName
- 06+2 NumberOfModuleForwarderRefs

D Delay imports

IMAGE_DELAY_IMPORT_DESCRIPTOR
- 00+4 dd grAttrs
- 04+4 szName
- 08+4 phmod
- 0c+4 pIAT
- 10+4 pINT
- 14+4 pBoundIAT
- 18+4 pUnloadIAT
- 1c+4 dwTimeStamp

E .NET

IMAGE_COR20_HEADER
- 00+4 cb
- 04+2 MajorRuntimeVersion
- 06+2 MinorRuntimeVersion
- 08+8 MetaData
- 10+4 Flags
- 14+4 EntryPointToken/RVA
- 18+8 Resources
- 20+8 StrongNameSignature
- 28+8 CodeManagerTable
- 30+8 VTableFixups
- 38+8 ExportAddressTableJumps
- 40+8 ManagedNativeHeader

METADATAHDR
- 00+4 Signature BSJB
- 04+2 MajorVersion
- 06+2 MinorVersion
- 08+4 Reserved
- 0c+4 VersionLength
- 10+? Version
- +2 Flags
- +2 Streams

METADATASTREAMHDR
- 00+4 offset
- 04+4 size
- 08+? string Stream name
- +? padding

METADATATABLESHDR
- 00+4 Reserved1
- 04+1 MajorVersion
- 05+1 MinorVersion
- 06+1 HeapOffsetSizes
- 07+1 Reserved2
- 08+8 MaskValid which tables are present
- 10+8 MaskSorted which tables are sorted
- 18+? NumRows[<64] how many rows in each table

Tables
- mdtModule
- mdtTypeRef
- mdtTypeDef
- mdtFieldDef
- mdtMethodDef
- mdtParamDef
- mdtMemberRef
- mdtCustomAttribute
- mdtAssembly
- mdtAssemblyRef

MODULETABLE
- 00+2 Generation
- 02+2 Name
- 04+2 Mvid
- 06+2 EncId
- 08+2 EncBaseId

TYPEREFTABLE
- 00+2 ResolutionScope
- 02+2 Name
- 04+2 Namespace

TYPEDEFTABLE
- 00+4 Flags
- 04+2 Name
- 06+2 Namespace
- 08+2 Extends
- 0a+2 FieldList
- 0c+2 MethodList

METHODDEFTABLE
- 00+4 RVA
- 04+2 ImplFlags
- 06+2 Flags
- 08+2 Name
- 0a+2 Signature
- 0c+2 ParamList

MEMBERREFTABLE
- 00+2 Class
- 02+2 Name
- 04+2 Signature

CUSTOMATTRIBUTETABLE
- 00+2 Parent
- 02+2 Type
- 04+2 Value

ASSEMBLYTABLE
- 00+4 HashAlgId
- 04+2 MajorVersion
- 06+2 MinorVersion
- 08+2 BuildNumber
- 0a+2 RevisionNumber
- 0c+4 Flags
- 10+2 PublicKey
- 12+2 Name
- 14+2 Culture

ASSEMBLYREFTABLE
- 00+2 MajorVersion
- 02+2 MinorVersion
- 04+2 BuildNumber
- 06+2 RevisionNumber
- 08+4 Flags
- 0c+2 PublicKeyOrToken
- 10+2 Name
- 12+2 Culture
- 14+2 HashValue

Disclaimer: this is only a subset of .Net structures — the required ones to make a working executable.

Resources (data itself)

strings
- 00+2 length null=no string
- 02+? string

Version information
VS_VERSION_INFO
- 00+2 wLength
- 02+2 wValueLength
- 04+02 wType   0:binary/text
- 06+2*? szKey[] 'VS_VERSION_INFO'
- +[0-3] Padding1
- ??+34 Value

VS_FIXEDFILEINFO
- 00+4 dwSignature 0xFEEF04BD
- 04+4 dwStrucVersion
- 08+4 dwFileVersionMS
- 0c+4 dwFileVersionLS
- 10+4 dwProductVersionMS
- 14+4 dwProductVersionLS
- 18+4 dwFileFlagsMask
- 1c+4 dwFileFlags
- 20+4 dwFileOS
- 24+4 dwFileType
- 28+4 dwFileSubtype
- 2c+4 dwFileDateMS
- 30+4 dwFileDateLS

- ??+[0-3] Padding2
- ??+? Children

StringFileInfo
- 00+2 wLength
- 02+2 wValueLength 0: no value
- 04+2 wType   0: children are binary
- 06+2*? szKey   'StringFileInfo'
- +[0-3] Padding
- ??+? Children

StringTable
- 00+2 wLength
- 02+2 wValueLength 0: no value
- 04+2 wType
- 06+2*? szKey 'language ID'
- +[0-3] Padding
- ??+? Children

String
- 00+2 wLength
- 02+2 wValueLength
- 04+2 wType
- 06+2*? szKey key:'ProductName'
- +[0-3] Padding
- +2*? Value[] str:'Notepad'

VarFileInfo
- 00+2 wLength
- 02+2 wValueLength 0 = no value
- 04+2 wType
- 06+2*? szKey 'VarFileInfo'
- +[0-3] Padding
- ??+? Children

Var
- 00+2 wLength
- 02+2 wValueLength
- 04+2 wType
- 06+2*? szKey 'Translation'
- +[0-3] Padding
- +4*? Value[]

Icons
<header-less .ICO data>

GRPICONDIR
- 00+2 idReserved
- 02+2 idType
- 04+2 idCount

GRPICONDIRENTRY
- 00+1 bWidth
- 01+1 bHeight
- 02+1 bColorCount
- 03+1 bReserved
- 04+2 wPlanes
- 06+2 wBitCount
- 08+4 dwBytesInRes
- 0c+2 nId

manifest (XML file)
<XML file>

Constants

File header
IMAGE_FILE_MACHINE_* — Machine
I386	014C
ARM7	01c4
AMD64	8664

IMAGE_FILE_* — Characteristics
RELOCS_STRIPPED	0001
EXECUTABLE_IMAGE	0002
LINE_NUMS_STRIPPED	0004
LOCAL_SYMS_STRIPPED	0008
LARGE_ADDRESS_AWARE	0020
32BIT_MACHINE	0100
DEBUG_STRIPPED	0200
DLL	2000

Optional Header
IMAGE_NT_OPTIONAL_HDR*_MAGIC — Magic
32	010b
64	020b

IMAGE_SUBSYSTEM_* — Subsystem
NATIVE (driver)	0001
WINDOWS_GUI	0002
WINDOWS_CUI (console)	0003

IMAGE_DLLCHARACTERISTICS_* — DllCharacteristics
DYNAMIC_BASE (aslr)	0040
NX_COMPAT (dep)	0100
NO_SEH	0400
TERMINAL_SERVER_AWARE	8000

Section
IMAGE_SCN_* — Characteristics
CNT_*	
CODE	00000020
INITIALIZED_DATA	00000040
UNINITIALIZED_DATA	00000080
MEM_*	
DISCARDABLE	02000000
SHARED (risky)	10000000
EXECUTE	20000000
READ	40000000
WRITE	80000000

Relocations
IMAGE_REL_BASED_* — TypeOffset
ABSOLUTE	0
HIGHLOW	3

Resources
RT_*	NameID
BITMAP	02
ICON	03
MENU	04
DIALOG	05
STRING	06
GROUP_ICON	0e
VERSION	10
MANIFEST	18

Legend
- Relative Virtual Address
- Virtual Address (requires relocation)
- offset
- relative offset