PE102

ortable xecutable

a Windows executable format overview

MZ DOS HEADER
PE HEADER
NT HEADERS
FILE HEADER
OPTIONAL HEADER
DATA DIRECTORY
EXPORT, IMPORT, ADDRESS TABLE
RESOURCES, EXCEPTIONS, RELOCATIONS
DEBUG, TLS, SAFESEH, .NET
SECTIONS

Ange Albertini
2009-2013 Corkami

HEADERS & SECTIONS

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

Constants

File header

IMAGE_FILE_MACHINE_*	Machine
I386	014c
ARMV7	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

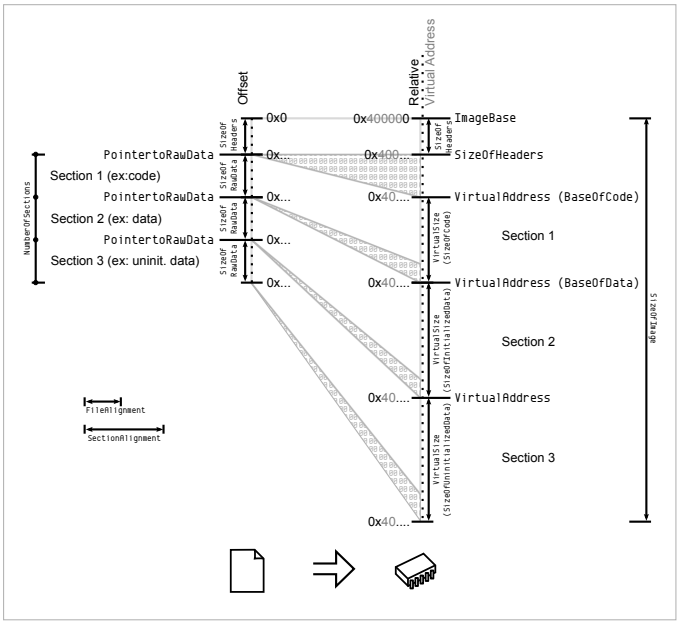
IMAGE_SCN_*	Characteristics
CNT_*	
CODE	00000020
INITIALIZED_DATA	00000040
UNINITIALIZED_DATA	00000080
MEM_*	
DISCARDABLE	02000000
SHARED (risky!)	10000000
EXECUTE	20000000
READ	40000000
WRITE	80000000

Relocations

IMAGE_REL_BASED_*	TypeOffset
ABSOLUTE	0
HIGHLOW	3

Resources

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



OFFSET 0 — DOS Header

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+2 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 00+2 Magic 32b or 64b
02+1 02+1 MajorLinkerVersion required with signatures
03+1 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 -2^y, with y≥x
24+4 24+4 FileAlignment -2^x
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 4:4W95 5:2k2000 6:2Vista
32+2 32+2 MinorSubsystemVersion
34+4 34+4 Win32VersionValue overrides OS values 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 ≤16
70+8 60+8 VirtualAddress, Size

SizeofOptionalHeader

Data Directories

IMAGE_DATA_DIRECTORY[]

NumberOfRvaAndSizes

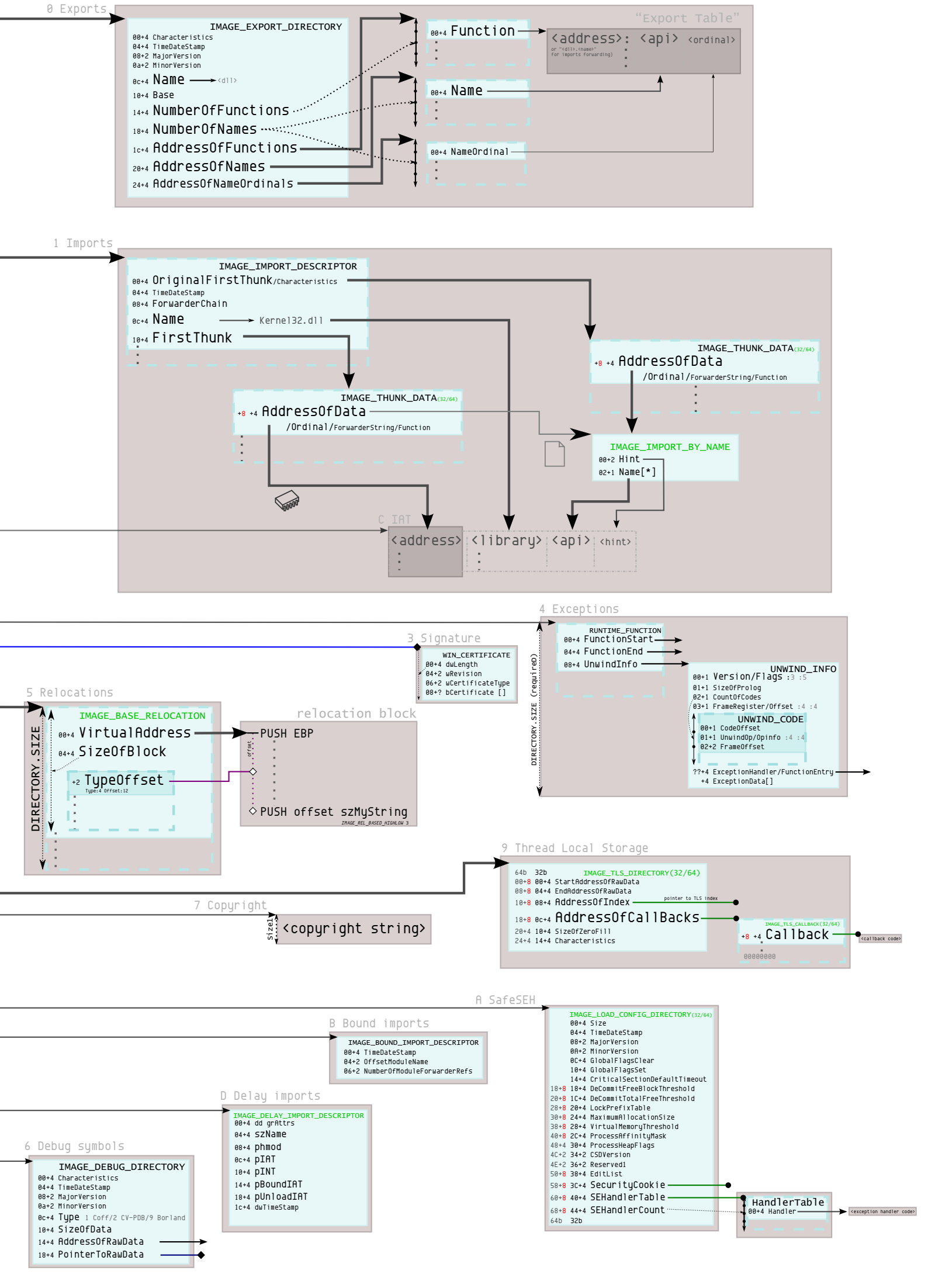
0 EXPORT
1 IMPORT
2 RESOURCE icons, manifest, version...
3 EXCEPTION 64bits exceptions
4 SECURITY Authenticode signature
5 BASERELOC relocations
6 DEBUG symbols
7 COPYRIGHT/Architecture useless
8 GLOBALPTR only on Itanium systems
9 TLS Thread Local Storage
A LOAD_CONFIG SafeSEH
B BOUND_IMPORT speeds up imports loading
C IAT Import Address table
D DELAY_IMPORT
E COM_DESCRIPTOR .NET header
F reserved unused
<ignored>...

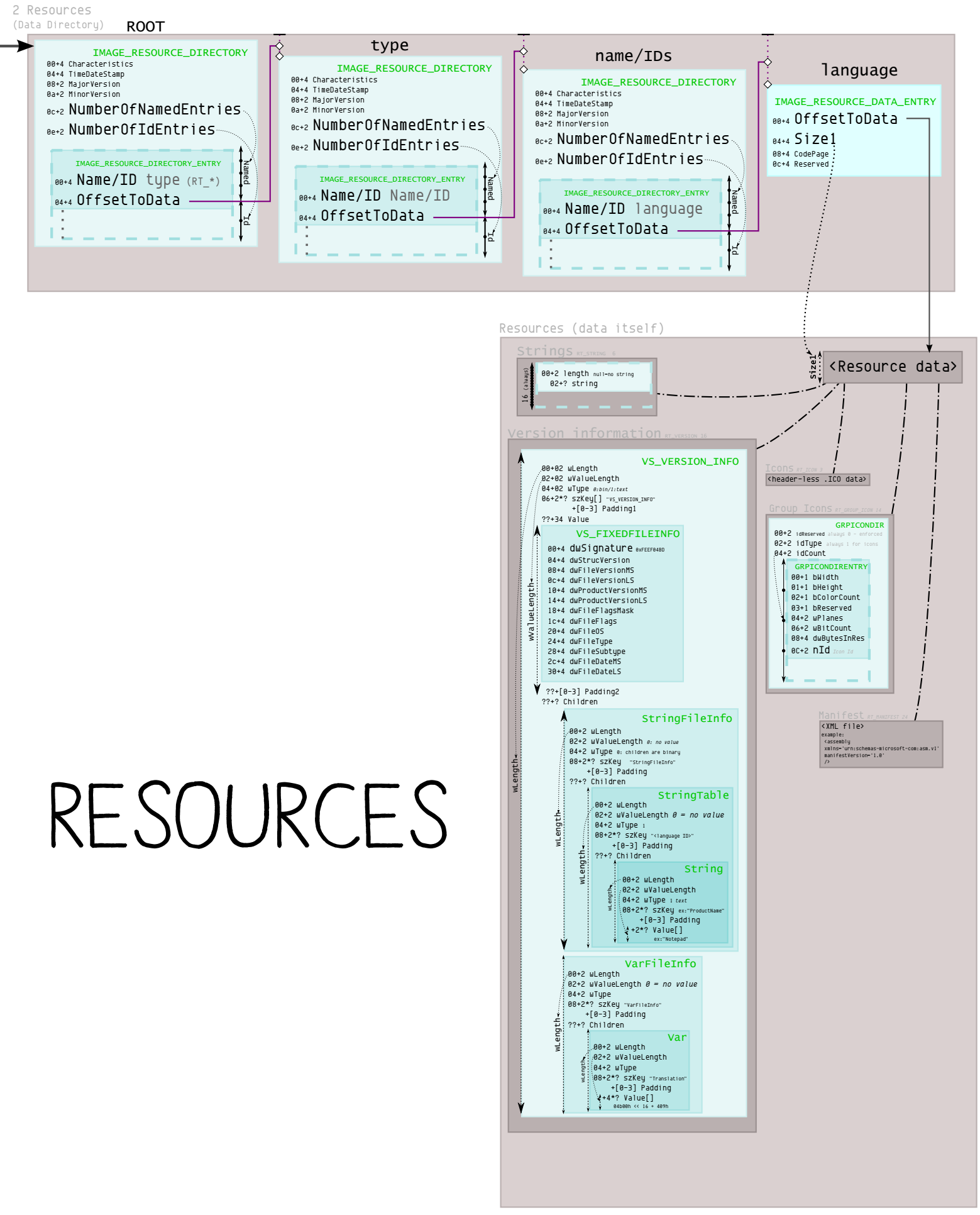
NumberOfSections

IMAGE_SECTION_HEADER

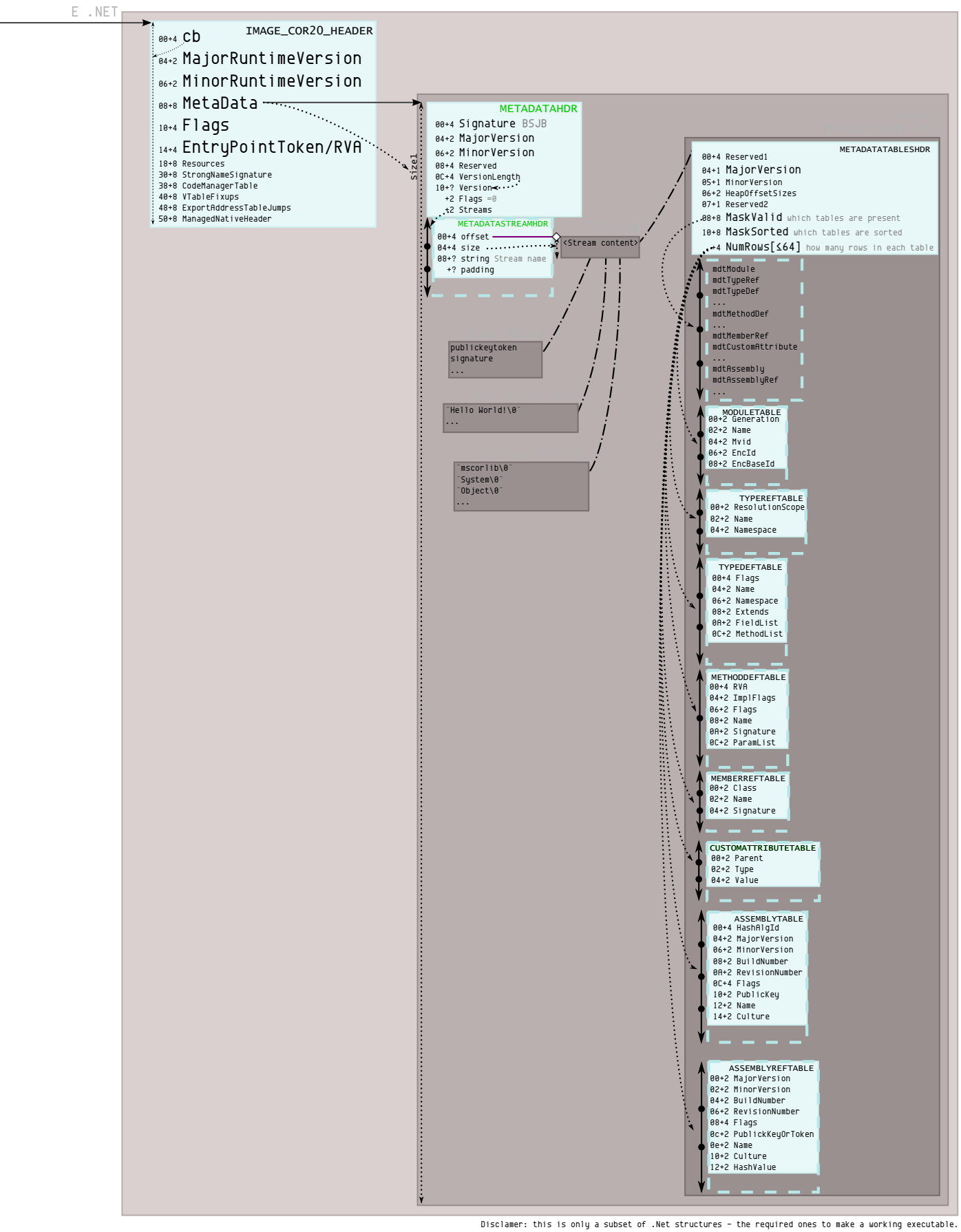
00+1 Name[8]
08+4 VirtualSize
0c+4 VirtualAddress → section start in memory
10+4 SizeOfRawData
14+4 PointerToRawData → section start in file
18+4 PointerToRelocations
1c+4 PointerToLinenumbers
20+2 NumberOfRelocations
22+2 NumberOfLinenumbers
24+4 Characteristics RWX

Section Table


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
00+4 Function
00+4 Name
00+4 NameOrdinal
"Export Table"
<address>: <api> <ordinal>
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_IMPORT_BY_NAME
00+2 Hint
02+1 Name[*]
C IAT
<address>
<library>
<api>
<hint>
4 Exceptions
RUNTIME_FUNCTION
00+4 FunctionStart
04+4 FunctionEnd
08+4 UnwindInfo
DIRECTORY.SIZE (required)
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
DIRECTORY.SIZE
relocation block
PUSH EBP
offset
PUSH offset szMyString
IMAGE_REL_BASED_HIGHLOW 3
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
IMAGE_TLS_CALLBACK(32/64)
+8 +4 Callback
<callback code>
00000000
7 Copyright
Size1
<copyright string>
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
4E+2 36+2 Reserved1
50+8 38+4 EditList
58+8 3C+4 SecurityCookie
60+8 40+4 SEHandlerTable
68+8 44+4 SEHandlerCount
64b 32b
HandlerTable
00+4 Handler
<exception handler code>
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
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


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
Named
Id
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
Named
Id
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
Named
Id
language
IMAGE_RESOURCE_DATA_ENTRY
00+4 OffsetToData
04+4 Size1
08+4 CodePage
0c+4 Reserved
Resources (data itself)
Strings RT_STRING 6
16 (always)
00+2 length null=no string
02+? string
Size1
<Resource data>
Version information RT_VERSION 16
VS_VERSION_INFO
00+02 wLength
02+02 wValueLength
04+02 wType 0:bin/1:text
06+2*? szKey[] "VS_VERSION_INFO"
+[0-3] Padding1
??+34 Value
wValueLength
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
wLength
StringFileInfo
00+2 wLength
02+2 wValueLength 0: no value
04+2 wType 0: children are binary
08+2*? szKey "StringFileInfo"
+[0-3] Padding
??+? Children
wLength
StringTable
00+2 wLength
02+2 wValueLength 0 = no value
04+2 wType 1
08+2*? szKey "<language ID>"
+[0-3] Padding
??+? Children
wLength
String
00+2 wLength
02+2 wValueLength
04+2 wType 1 text
08+2*? szKey ex:"ProductName"
+[0-3] Padding
+2*? Value[]
ex:"Notepad"
VarFileInfo
00+2 wLength
02+2 wValueLength 0 = no value
04+2 wType
08+2*? szKey "VarFileInfo"
+[0-3] Padding
??+? Children
wLength
Var
00+2 wLength
02+2 wValueLength
04+2 wType
08+2*? szKey "Translation"
+[0-3] Padding
+4*? Value[]
04b00h << 16 + 409h
Icons RT_ICON 3
<header-less .ICO data>
Group Icons RT_GROUP_ICON 14
GRPICONDIR
00+2 idReserved always 0 - enforced
02+2 idType always 1 for icons
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 Icon Id
Manifest RT_MANIFEST 24
<XML file>
example:
<assembly
xmlns='urn:schemas-microsoft-com:asm.v1'
manifestVersion='1.0'
/>

RESOURCES



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

.NET