

# WINDOWS EXECUTABLE

## 32bit for Windows 95 and Windows NT

### *Technical File Information:*

#### Image File Header

*Signature:* 00004550  
*Machine:* Intel 386  
*Number of Sections:* 0008  
*Time Date Stamp:* 453cd66c  
*Symbols Pointer:* 001c9400  
*Number of Symbols:* 000016d2  
*Size of Optional Header:* 00e0  
*Characteristics:* Relocation info stripped from file.  
File is executable (i.e. no unresolved external references).  
Line numbers stripped from file.  
32 bit word machine.

#### Image Optional Header

*Magic:* 010b  
*Linker Version:* 2.56  
*Size of Code:* 00040c00  
*Size of Initialized Data:* 00044800  
*Size of Uninitialized Data:* 00004c00  
*Address of Entry Point:* 00001240  
*Base of Code:* 00001000  
*Base of Data:* 00042000  
*Image Base:* 00400000  
*Section Alignment:* 00001000  
*File Alignment:* 00000200  
*Operating System Version:* 4.00  
*Image Version:* 1.00  
*Subsystem Version:* 4.00  
*Reserved1:* 00000000  
*Size of Image:* 001d2000  
*Size of Headers:* 00000400  
*Checksum:* 00203eeb  
*Subsystem:* Image runs in the Windows GUI subsystem.  
*DLL Characteristics:* 0000  
*Size of Stack Reserve:* 00200000  
*Size of Stack Commit:* 00001000  
*Size of Heap Reserve:* 00100000  
*Size of Heap Commit:* 00001000  
*Loader Flags:* 00000000  
*Size of Data Directory:* 00000010  
*Import Directory Virtual Address:* 0004b000  
*Import Directory Size:* 00000e00  
*Resource Directory*

Virtual Address: 0004c000  
Resource Directory Size: 0000028c

### Import Table

COMCTL32.DLL

Ordinal Function Name

005b InitCommonControls

GDI32.dll

Ordinal Function Name

000c BitBlt  
0020 CreateCompatibleBitmap  
0021 CreateCompatibleDC  
0039 CreatePen  
0042 CreateSolidBrush  
0045 DeleteDC  
0048 DeleteObject  
00e3 LineTo  
00e6 MoveToEx  
0115 SelectObject

KERNEL32.dll

Ordinal Function Name

0001 AddAtomA  
0026 CloseHandle  
0044 CreateFileA  
0057 CreateSemaphoreA  
005a CreateThread  
006a DeleteCriticalSection  
007d EnterCriticalSection  
009b ExitProcess  
009c ExitThread  
00af FindAtomA  
00dc GetAtomNameA  
00ec GetCommandLineA  
0143 GetLastError  
014f GetModuleHandleA  
0180 GetStartupInfoA  
01ea InitializeCriticalSection  
01ee InterlockedDecrement  
01f2 InterlockedIncrement  
0209 LeaveCriticalSection  
0272 ReleaseSemaphore  
027d ResumeThread  
02c5 SetLastError

02df SetUnhandledExceptionFilter  
02eb Sleep  
02f4 TerminateThread  
02f7 TlsAlloc  
02f8 TlsFree  
02f9 TlsGetValue  
02fa TlsSetValue  
0325 WaitForSingleObject  
0336 WriteFile  
0360 lstrlenA

msvcrt.dll

Ordinal            Function Name

0018 \_fdopen  
0041 \_read  
0054 \_strdup  
0071 \_write

msvcrt.dll

Ordinal            Function Name

0027 \_\_getmainargs  
0030 \_\_mb\_cur\_max  
003c \_\_p\_\_environ  
003e \_\_p\_\_fmode  
0050 \_\_set\_app\_type  
006f \_assert  
0079 \_cexit  
008d \_ctype  
0098 \_errno  
00ad \_filelengthi64  
00c2 \_fstati64  
00e9 \_iob  
00eb \_isctype  
011c \_lseeki64  
015e \_onexit  
0167 \_pctype  
0184 \_setmode  
019f \_strnicmp  
01bd \_vsprintf  
0215 abort  
021c atexit  
022a exit  
022d fclose  
0230 fflush  
0232 fgetpos  
0238 fopen  
0239 fprintf  
023e fread  
023f free  
0244 fsetpos

0247	fwrite
0249	getc
026d	localeconv
0272	malloc
0276	memchr
0278	memcpy
0279	memmove
027a	memset
0280	putc
028e	setlocale
028f	setvbuf
0290	signal
0293	sprintf
0299	strcmp
029a	strcoll
029b	strcpy
029e	strftime
029f	strlen
02a7	strtod
02ab	strxfrm
02b8	ungetc

USER32.dll

<u>Ordinal</u>	<u>Function Name</u>
----------------	----------------------

004f	CreateDialogParamA
0059	CreateWindowExA
008f	DestroyWindow
0094	DispatchMessageA
00b3	EnableWindow
00d0	FillRect
00eb	GetClientRect
00fc	GetDlgItem
0124	GetMessageA
0152	GetWindowDC
0154	GetWindowLongA
016f	InvalidateRect
017d	IsDialogMessageA
0186	IsWindow
018c	KillTimer
01ae	MessageBoxA
01d0	PostQuitMessage
01e6	ReleaseDC
01f4	SendMessageA
022b	SetTimer
0241	ShowWindow
0258	TranslateMessage
0264	UpdateWindow

### **Section Table**

*Section name:* .text

*Virtual Size:* 00040bdc  
*Virtual Address:* 00001000  
*Size of raw data:* 00040c00  
*Pointer to Raw Data:* 00000400  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains code  
Section contains initialized data  
Section is executable  
Section is readable

*Section name:* .data  
*Virtual Size:* 00000190  
*Virtual Address:* 00042000  
*Size of raw data:* 00000200  
*Pointer to Raw Data:* 00041000  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains initialized data  
Section is readable  
Section is writeable

*Section name:* .rdata  
*Virtual Size:* 000027f4  
*Virtual Address:* 00043000  
*Size of raw data:* 00002800  
*Pointer to Raw Data:* 00041200  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains initialized data  
Section is readable

*Section name:* .bss  
*Virtual Size:* 00004c00  
*Virtual Address:* 00046000  
*Size of raw data:* 00000000  
*Pointer to Raw Data:* 00000000  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains uninitialized data

Section is readable  
Section is writeable

*Section name:* .idata  
*Virtual Size:* 00000e00  
*Virtual Address:* 0004b000  
*Size of raw data:* 00000e00  
*Pointer to Raw Data:* 00043a00  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains initialized data  
Section is readable  
Section is writeable

*Section name:* .rsrc  
*Virtual Size:* 0000028c  
*Virtual Address:* 0004c000  
*Size of raw data:* 00000400  
*Pointer to Raw Data:* 00044800  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contains initialized data  
Section is readable  
Section is writeable

*Section name:* .stab  
*Virtual Size:* 0001e714  
*Virtual Address:* 0004d000  
*Size of raw data:* 0001e800  
*Pointer to Raw Data:* 00044c00  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contents will not become part of image  
Section can be discarded  
Section is readable

*Section name:* .stabstr<sup>^</sup>  
*Virtual Size:* 00165e6c  
*Virtual Address:* 0006c000  
*Size of raw data:* 00166000

*Pointer to Raw Data:* 00063400  
*Pointer to Relocations:* 00000000  
*Pointer to Line Numbers:* 00000000  
*Number of Relocations:* 0000  
*Number of Line Numbers:* 0000  
*Characteristics:* Section contents will not become part of image  
Section can be discarded  
Section is readable

### **Header Information**

*Signature:* 5a4d  
*Last Page Size:* 0090  
*Total Pages in File:* 0003  
*Relocation Items:* 0000  
*Paragraphs in Header:* 0004  
*Minimum Extra Paragraphs:* 0000  
*Maximum Extra Paragraphs:* ffff  
*Initial Stack Segment:* 0000  
*Initial Stack Pointer:* 00b8  
*Complemented Checksum:* 0000  
*Initial Instruction Pointer:* 0000  
*Initial Code Segment:* 0000  
*Relocation Table Offset:* 0040  
*Overlay Number:* 0000  
*Reserved:* 0000 0000 0000 0000  
0000 0000 0000 0000  
0000 0000 0000 0000  
0000 0000 0000 0000  
*Offset to New Header:* 00000080  
*Memory Needed:* 2K