WINDOWS EXECUTABLE
32bit for Windows 95 and Windows NT

Technical File Information:

Image File Header

```
              Signature:  00004550
                Machine:  Intel 386
     Number of Sections:  0006
        Time Date Stamp:  5a10ad86
        Symbols Pointer:  00000000
      Number of Symbols:  00000000
 Size of Optional Header  00e0
        Characteristics:

                          File is executable  (i.e. no unresolved external references).
                          32 bit word machine.
```

Image Optional Header

```
                  Magic:  010b
         Linker Version:  14.11
           Size of Code:  00049a00
Size of Initialized Data:     00029800
Size of Uninitialized Data:   00000000
 Address of Entry Point:  0002e2a6
           Base of Code:  00001000
           Base of Data:  0004b000
             Image Base:  00400000
      Section Alignment:  00001000
         File Alignment:  00000200
Operating System Version:     5.01
          Image Version:  0.00
       Subsystem Version:  5.01
              Reserved1:  00000000
           Size of Image:  00077000
         Size of Headers:  00000400
                Checksum:  006d7816
               Subsystem:  Image runs in the Windows GUI subsystem.
    DLL Characteristics:  33088
  Size of Stack Reserve:  00100000
   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:   000686b4
 Import Directory Size:   000000b4
     Resource Directory
       Virtual Address:   0006d000
Resource Directory Size:      00005f54
```

```
Security Directory Virtual Address:       006c6c88
Security Directory Size:      00002830
  Base Relocation Table
       Virtual Address:   00073000
Base Relocation Table Size:   00003dfc
Debug Directory Virtual Address:    00067650
  Debug Directory Size:   00000054
TLS Directory Virtual Address:      000676a4
    TLS Directory Size:   00000018
Load Configuration Directory Virtual Address:   00067030
Load Configuration Directory Size:        00000040
```

Import Table

```
      ADVAPI32.dll
      OrdinalFunction Name

      0230  RegCloseKey
      0261  RegOpenKeyExW
      01f7  OpenProcessToken
      001f  AdjustTokenPrivileges
      0197  LookupPrivilegeValueW
      017d  InitiateSystemShutdownExW
      0165  GetUserNameW
      026e  RegQueryValueExW
      0248  RegDeleteValueW
      0056  CloseEventLog
      01f6  OpenEventLogW
      028f  ReportEventW
      0072  ConvertStringSecurityDescriptorToSecurityDescriptorW
      00d8  DecryptFileW
      0083  CreateWellKnownSid
      0176  InitializeAcl
      02a6  SetEntriesInAclW
      0050  ChangeServiceConfigW
      0057  CloseServiceHandle
      005c  ControlService
      01f9  OpenSCManagerW
      01fb  OpenServiceW
      0228  QueryServiceStatus
      02b1  SetNamedSecurityInfoW
      0051  CheckTokenMembership
      0020  AllocateAndInitializeSid
      02a5  SetEntriesInAclA
      02b7  SetSecurityDescriptorGroup
      02b8  SetSecurityDescriptorOwner
      02b6  SetSecurityDescriptorDacl
      0177  InitializeSecurityDescriptor
      027e  RegSetValueExW
      0268  RegQueryInfoKeyW
      0252  RegEnumValueW
      024f  RegEnumKeyExW
      0244  RegDeleteKeyW
```

```
0239  RegCreateKeyExW
015a  GetTokenInformation
00b6  CryptDestroyHash
00c8  CryptHashData
00b3  CryptCreateHash
00c4  CryptGetHashParam
00cb  CryptReleaseContext
00b1  CryptAcquireContextW
0224  QueryServiceConfigW


USER32.dll
Ordinal     Function Name

0233  PeekMessageW
0236  PostMessageW
01db  IsWindow
0326  WaitForInputIdle
0237  PostQuitMessage
015d  GetMessageW
02fc  TranslateMessage
021c  MsgWaitForMultipleObjects
0239  PostThreadMessageW
015f  GetMonitorInfoW
0218  MonitorFromPoint
01cd  IsDialogMessageW
01eb  LoadCursorW
01e7  LoadBitmapW
02c4  SetWindowLongW
0196  GetWindowLongW
0120  GetCursorPos
0215  MessageBoxW
006e  CreateWindowExW
0306  UnregisterClassW
024e  RegisterClassW
009c  DefWindowProcW
00af  DispatchMessageW


OLEAUT32.dll
Ordinal     Function Name


GDI32.dll
Ordinal     Function Name

00e3  DeleteDC
00e6  DeleteObject
0277  SelectObject
02b3  StretchBlt
01fd  GetObjectW
0030  CreateCompatibleDC


SHELL32.dll
```

Ordinal	Function Name
0006	CommandLineToArgvW
00c3	SHGetFolderPathW
0121	ShellExecuteExW

ole32.dll

Ordinal	Function Name
006c	CoUninitialize
003f	CoInitializeEx
003e	CoInitialize
0179	StringFromGUID2
0010	CoCreateInstance
0068	CoTaskMemFree
0006	CLSIDFromProgID
0040	CoInitializeSecurity

KERNEL32.dll

Ordinal	Function Name
0186	GetCommandLineA
0172	GetCPInfo
0237	GetOEMCP
0052	CloseHandle
008f	CreateFileW
0245	GetProcAddress
0348	LocalFree
02d3	HeapSetInformation
0202	GetLastError
0218	GetModuleHandleW
015e	FormatMessageW
054d	lstrlenA
054e	lstrlenW
0367	MultiByteToWideChar
0511	WideCharToMultiByte
032d	LCMapStringW
04b2	Sleep
0203	GetLocalTime
0214	GetModuleFileNameW
011d	ExpandEnvironmentStringsW
0285	GetTempPathW
0283	GetTempFileNameW
0081	CreateDirectoryW
01fb	GetFullPathNameW
0064	CompareStringW
01c1	GetCurrentProcessId
0525	WriteFile
0466	SetFilePointer
033f	LoadLibraryW
0270	GetSystemDirectoryW
0088	CreateFileA
02cb	HeapAlloc
02d2	HeapReAlloc

```
02cf  HeapFree
02d4  HeapSize
024a  GetProcessHeap
012e  FindClose
0187  GetCommandLineW
01bf  GetCurrentDirectoryW
0403  RemoveDirectoryW
0461  SetFileAttributesW
01ea  GetFileAttributesW
00d6  DeleteFileW
0139  FindFirstFileW
0145  FindNextFileW
0360  MoveFileExW
01c0  GetCurrentProcess
01c5  GetCurrentThreadId
02e2  InitializeCriticalSection
00d1  DeleteCriticalSection
03fa  ReleaseMutex
04c5  TlsAlloc
04c7  TlsGetValue
04c8  TlsSetValue
04c6  TlsFree
00a8  CreateProcessW
02a4  GetVersionExW
04e4  VerSetConditionMask
0162  FreeLibrary
00ee  EnterCriticalSection
0339  LeaveCriticalSection
0277  GetSystemTime
0225  GetNativeSystemInfo
0217  GetModuleHandleExW
02af  GetWindowsDirectoryW
027e  GetSystemWow64DirectoryW
01da  GetEnvironmentStringsW
04e8  VerifyVersionInfoW
02ab  GetVolumePathNameW
01c8  GetDateFormatW
029e  GetUserDefaultUILanguage
026c  GetSystemDefaultLangID
029c  GetUserDefaultLangID
0269  GetStringTypeW
03c0  ReadFile
0467  SetFilePointerEx
00e8  DuplicateHandle
02ec  InterlockedExchange
02e9  InterlockedCompareExchange
033e  LoadLibraryExW
0085  CreateEventW
0399  ProcessIdToSessionId
0380  OpenProcess
024c  GetProcessId
04f9  WaitForSingleObject
0065  ConnectNamedPipe
047c  SetNamedPipeHandleState
00a0  CreateNamedPipeW
00b5  CreateThread
```

```
01e0  GetExitCodeThread
0459  SetEvent
04f7  WaitForMultipleObjects
02ef  InterlockedIncrement
02eb  InterlockedDecrement
040f  ResetEvent
0453  SetEndOfFile
046a  SetFileTime
0346  LocalFileTimeToFileTime
00e4  DosDateTimeToFileTime
0061  CompareStringA
01df  GetExitCodeProcess
0493  SetThreadExecutionState
0072  CopyFileExW
0357  MapViewOfFile
04d6  UnmapViewOfFile
009e  CreateMutexW
008c  CreateFileMappingW
028c  GetThreadLocale
030a  IsValidCodePage
0134  FindFirstFileExW
0161  FreeEnvironmentStringsW
0487  SetStdHandle
019a  GetConsoleCP
01ac  GetConsoleMode
0157  FlushFileBuffers
00ca  DecodePointer
0524  WriteConsoleW
0215  GetModuleHandleA
02b3  GlobalAlloc
02ba  GlobalFree
01f1  GetFileSizeEx
0075  CopyFileW
04e9  VirtualAlloc
04ec  VirtualFree
04be  SystemTimeToTzSpecificLocalTime
0298  GetTimeZoneInformation
04bd  SystemTimeToFileTime
0273  GetSystemInfo
04ef  VirtualProtect
04f1  VirtualQuery
018f  GetComputerNameW
044d  SetCurrentDirectoryW
01f3  GetFileType
0168  GetACP
0119  ExitProcess
0264  GetStdHandle
02e3  InitializeCriticalSectionAndSpinCount
0473  SetLastError
0418  RtlUnwind
04d3  UnhandledExceptionFilter
04a5  SetUnhandledExceptionFilter
04c0  TerminateProcess
0304  IsProcessorFeaturePresent
03a7  QueryPerformanceCounter
0279  GetSystemTimeAsFileTime
```

```
      02e7  InitializeSListHead
      0300  IsDebuggerPresent
      0263  GetStartupInfoW
      03b1  RaiseException
      033d  LoadLibraryExA


      RPCRT4.dll
      Ordinal     Function Name

      01fb  UuidCreate
```

Section Table

```
           Section name:  .text
           Virtual Size:  00049937
         Virtual Address:  00001000
       Size of raw data:  00049a00
    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 is executable
                          Section is readable
```

```
           Section name:  .rdata
           Virtual Size:  0001ed60
         Virtual Address:  0004b000
       Size of raw data:  0001ee00
    Pointer to Raw Data:  00049e00
 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:  .data
           Virtual Size:  00001730
         Virtual Address:  0006a000
       Size of raw data:  00000a00
    Pointer to Raw Data:  00068c00
 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:  .wixburn
          Virtual Size:  00000038
       Virtual Address:  0006c000
     Size of raw data:  00000200
   Pointer to Raw Data:  00069600
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:  .rsrc
          Virtual Size:  00005f54
       Virtual Address:  0006d000
     Size of raw data:  00006000
   Pointer to Raw Data:  00069800
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:  .reloc
          Virtual Size:  00003dfc
       Virtual Address:  00073000
     Size of raw data:  00003e00
   Pointer to Raw Data:  0006f800
Pointer to Relocations:  00000000
Pointer to Line Numbers:  00000000
  Number of Relocations:  0000
Number of Line Numbers:  0000
       Characteristics:  Section contains initialized data
                         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:  00000110
          Memory Needed:  2K
```