



PEBrowse Professional Windows Disassembler

Microsoft® Private Cloud
Increase Your VM Density Without
Increasing Cost. Learn More Today!
Microsoft.com/readynow

Home	FAQ	News	Software	Documentation	SiteSearch
------	-----	------	----------	---------------	------------

Like 26

PEBrowse Professional (v10.1.4) is a static-analysis tool and disassembler for Win32/Win64 executables and Microsoft .NET assemblies produced according to the Portable Executable specifications published by Microsoft. For Microsoft Windows 7, Windows Vista, Windows XP, Windows 2000, and others. **PEBrowse64 Professional** (v2.1) is a rewrite of PEBrowse Professional but is a 64-bit executable and requires the .NET framework. It will display only Win64 executables, native, managed and mixed.

With the PEBrowse disassembler, one can open and examine any executable without the need to have it loaded as part of an active process with a debugger. Applications, system DLLs, device-drivers and Microsoft .NET assemblies are all candidates for offline analysis using either PEBrowse programs. The information is organized in a convenient treeview index with the major divisions of the PE file displayed as nodes. In most cases selecting nodes will enable context-sensitive multiple view menu options, including binary dump, section detail, disassembly and structure options as well as displaying sub-items, such as optional header directory entries or exported functions, that can be found as part of a PE file unit. Several table displays, hex/ASCII equivalents, window messages and error codes, as well as a calculator and scratchpads are accessible from the main menu (calculator, messages and codes in PEBrowse Professional only).

While the binary dump display offers various display options, e.g., BYTE, WORD, or DWORD alignment, the greatest value of PEBrowse comes when one disassembles an entry-point. An entry-point in PEBrowse is defined as:

- module entry-point
 - exports (if any)
- debug-symbols (if a valid PDB, i.e., program database file, is present)
 - imported API references
- relocation addresses
 - internal functions/subroutines
 - any valid address inside of the module

Selecting and disassembling any number of these entry-points produces a versatile display rich in detail including upper/lowercase display, C/Pascal/Assembler suffix/prefixing, object code, color-coded statements, register usage highlighting, and jump/call target preview popups. Additional information, such as variable and function names, will also be present if one has access to a valid PDB file. Disassembly comes in two flavors: linear sweep (sequential disassembly from a starting address) and recursive traversal, aka, analysis mode (disassembly of all statements reachable by non-call statements - extended analysis disassembles all internal call statements as well). The latter mode also presents local variables with cross-referencing, highlighting, and renaming options. If one adds/changes variable name or adds comments to specific lines, these can be displayed in a session file which will record and save all currently opened displays.

PEBrowse Professional will decompile type library information either embedded inside of the binary as the resource "TYPELIB" or inside of individual type libraries, i.e., .TLB or .OLB files. PEBrowse Professional and PEBrowse64 Professional also display all metadata for .NET assemblies and displays IL (Intermediate Language) for .NET methods. They seamlessly handle mixed assemblies, i.e., those that contain both native and managed code. Finally, the 32-bit PEBrowse can be employed as a file browse utility for any type of file with the restriction that the file must be small enough that it can be memory-mapped.

Screenshot of PEBrowse Professional:

ntdll.dll - PEBrowse Professional

File Edit View Tools Window Help

DOS Header
File Header
Optional Header
Sections
 .text
 ECCODE
 .data
 .rsrc
 .reloc
Exports
Resources
Debug
 CodeView
 Debug Symbols

Disassembly of Function: LdrLockLoaderLock@12 + 0x00FA (0x77F52D14)

ARG/VAR/SYM	Characteristics	References
EBP+0x10		0x77F52DC9
EBP+0x8		0x77F52DD2
EBP+0xC		0x77F52DBC
EBP-0x1C		0x77F725C8

Number of Parameters: 3
Locals Variables Size (in BYTES): 40 (0x00000028)
Registers Saved: 3
Prologue Size (in BYTES): 12 (0x0C)
Size of Routine: 469
NONFPD Frame

```

;*****
; LdrLockLoaderLock (67)
SYN: LdrLockLoaderLock@12
0x77F52DAA: 6A14      PUSH     0x14
0x77F52DAC: 6860D6F677 PUSH     0x77F6D660      ; CODE(1):0xFF 0xFF 0xFF 0x
0x77F52DB1: B85F580200 CALL     _SEH_prolog      ; (0x77F78C15)
; end of prologue
0x77F52DB6: 8A1DC030FC77 MOV     BL,DWORD PTR [LdrpInLdrInit]; (0x77FC30C0)
0x77F52DBC: 8B750C      MOV     ESI,DWORD PTR [EBP+0xC]
0x77F52DBF: 33D2      XOR     EDI,EDI
0x77F52DC1: 3BF2      CMP     ESI,EDI
0x77F52DC3: 0F85460F0200 JNE     0x77F73D0F      ; (*+0x20F4C)
0x77F52DC9: 8B7D10      MOV     EDI,DWORD PTR [EBP+0x10] ; <=0x77F73D11(*+0x20F4B)
  
```

ANALYZE Line 18 of 135

Analysis of Debug Symbol: LdrLockLoaderLock@12 (0x77F52D14)

```

0x77F52DAA: PUSH     0x14
0x77F52DAC: PUSH     0x77F6D660
0x77F52DB1: CALL     _SEH_prolog
0x77F52DB6: MOV     BL,DWORD PTR [0x77FC30C0]
0x77F52DBC: MOV     ESI,DWORD PTR [EBP+0xC]
0x77F52DBF: XOR     EDI,EDI
0x77F52DC1: CMP     ESI,EDI
0x77F52DC3: JNE     0x77F73D0F
0x77F52DC9: MOV     EDI,DWORD PTR [EBP+0x10]
0x77F52DCC: CMP     EDI,EDI
0x77F52DCE: JE      0x77F52DD2
0x77F52DD0: MOV     DWORD PTR [EDI],EDI
  
```

1290 Subroutines Discovered By G158 Call-Chain-Scanner

- _LdrLoadDll@16 (0x77F55669) - 5 Items
- _LdrLockLoaderLock@12 (0x77F52DAA) - 13 Items
 - _LdrAddRefDll@8 + 0x0035 (0x77F8F547)
 - _LdrDisableThreadCalloutsForDll@4 - 0x0462 (0x77F5AA80)
 - _LdrEnumerateLoadedModules@12 + 0x0027 (0x77F5B93A)
 - _LdrFlushAlternateResourceModules@0 + 0x0018 (0x77F70DE7)
 - _LdrGetDllHandleEx@20 + 0x007A (0x77F548D0)
 - _LdrInitShimEngineDynamic@4 + 0x0010 (0x77F8F75C)
 - _LdrLoadAlternateResourceModule@8 + 0x2167B (0x77F80E55)
 - _LdrLoadDll@16 + 0x0076 (0x77F556DF)
 - _LdrSetAppCompatDllRedirectionCallback@12 + 0x0024 (0x77F8F5F7)
 - _LdrUnloadAlternateResourceModule@4 + 0x0018 (0x77F5FCF3)
 - _RtlPcToFileHeader@8 + 0x001B (0x77F6FCE9)
 - _RtlQueryInformationActivationContext@28 + 0x19F20 (0x77F6FC6F)
 - _RtlQueryInformationActivationContext@28 + 0x2A05C (0x77F7FDA8)
- _LdrAccessResourceData@16 (0x77F57444) - 5 Items

EXACT SYMBOLS DEFAULT

[Download PEBrowse Professional.](#)

[Download PEBrowse64 Professional.](#)

[Read the Tutorial.](#)



Home | [FAQ](#) | [News](#) | [Software](#) | [Documentation](#) | [SiteSearch](#) | [Licensing](#) | [Links](#) | [SiteIndex](#) | [AboutUs](#) | [ContactUs](#)
 Page best viewed at 1024x768. Page last updated 2011-07-10. This site is PIKT® powered.
 Copyright © 1998-2011 Russell Osterlund. All rights reserved. SmidgeonSoft is a wholly-owned division of SmidgeonSoft, LLC.