<table>
<tr><th colspan="13">PEB Evolution</th></tr>
<tr><td>NTDLL TimeStamp</td><td>3B7D7EBB
3B7DE01E
3D6DD030
3D6DE29B</td><td>41107F17
411089B7
48025C72
4802B3E6
498C7036</td><td>3E8004ED
3E800DDD</td><td>42435C02
42435C4D
42435E08
424360CC
45D69A63
45D6A034
45D70A62
45D70BAD</td><td>4549AB99
4549AB99
4549ACCF
4549ACD4
4549B0A8
4549B414</td><td>47918547
47918548
47918A5E
47918A66
47918DFE
4791909A
49E018CF
49E018CF
49E018FF
49E01904
49E02292
49E02503</td><td>4943158F
494316C4
49431951
49431F6B</td><td>49EE8A5F
49EE8E6C
49EE9768
49EE9FA1
4A5BBF34
4A5BC19D
4A5BC487
4A5BCCA6
4BA9775A
4BA9796A
4CC78DE7
4CE77482
4CE78918
4CE7891C
4CE78F28
4CE79326
4EC47C8E
4EC48464</td><td>4E546498
4E5464A2
4E54669B</td><td>4F3F1DFC
4F3F1DFC
4F3F2277
4F3F2BEC
4F3F36C6
4F3F373D</td><td>4FB70542
4FB70543
4FB70C03
4FB7166D
4FB71A7F
4FB71ABD
50109933
50109933
50109E76
5010ACD2
5010AE7A
5010AEB6</td><td>ReWolf</td></tr>
<tr><th>OS Version</th><th>XP, XP SP1</th><th>XP SP2, XP SP3</th><th>2003</th><th>2003 SP1, 2003 SP2</th><th>Vista</th><th>Vista SP1, Vista SP2</th><th>Win7 Beta</th><th>Win7 RC, Win7 RTM</th><th>Win8 Dev Prev x64 (8102)</th><th>Win8 Beta</th><th>Win8 RC, Win8 RTM</th><th></th></tr>
<tr><th>x86 offset
offset:bit(len)</th><th colspan="11">Field Name</th><th>x64 offset
offset:bit(len)</th></tr>
<tr><td>0x0000</td><td colspan="11">unsigned char, InheritedAddressSpace</td><td>0x0000</td></tr>
<tr><td>0x0001</td><td colspan="11">unsigned char, ReadImageFileExecOptions</td><td>0x0001</td></tr>
<tr><td>0x0002</td><td colspan="11">unsigned char, BeingDebugged</td><td>0x0002</td></tr>
<tr><td>0x0003</td><td colspan="3" rowspan="9">unsigned char, SpareBool</td><td colspan="8">unsigned char, BitField</td><td>0x0003</td></tr>
<tr><td>0x0003:0x00(1)</td><td colspan="8">unsigned char, ImageUsesLargePages</td><td>0x0003:0x00(1)</td></tr>
<tr><td>0x0003:0x01(1)</td><td rowspan="7">unsigned char, SpareBits</td><td colspan="7">unsigned char, IsProtectedProcess</td><td>0x0003:0x01(1)</td></tr>
<tr><td>0x0003:0x02(1)</td><td colspan="7">unsigned char, IsLegacyProcess</td><td>0x0003:0x02(1)</td></tr>
<tr><td>0x0003:0x03(1)</td><td colspan="7">unsigned char, IsImageDynamicallyRelocated</td><td>0x0003:0x03(1)</td></tr>
<tr><td>0x0003:0x04(1)</td><td rowspan="4">unsigned char, SpareBits</td><td colspan="6">unsigned char, SkipPatchingUser32Forwarders</td><td>0x0003:0x04(1)</td></tr>
<tr><td>0x0003:0x05(1)</td><td colspan="4" rowspan="3">unsigned char, SpareBits</td><td colspan="2">unsigned char, IsPackagedProcess</td><td>0x0003:0x05(1)</td></tr>
<tr><td>0x0003:0x06(1)</td><td rowspan="2">unsigned char, SpareBits</td><td>unsigned char, IsAppContainer</td><td>0x0003:0x06(1)</td></tr>
<tr><td>0x0003:0x07(1)</td><td>unsigned char, SpareBits</td><td>0x0003:0x07(1)</td></tr>
<tr><td>0x0004</td><td colspan="11">void *, Mutant</td><td>0x0008</td></tr>
<tr><td>0x0008</td><td colspan="11">void *, ImageBaseAddress</td><td>0x0010</td></tr>
<tr><td>0x000C</td><td colspan="11">struct _PEB_LDR_DATA *, Ldr</td><td>0x0018</td></tr>
<tr><td>0x0010</td><td colspan="11">struct _RTL_USER_PROCESS_PARAMETERS *, ProcessParameters</td><td>0x0020</td></tr>
<tr><td>0x0014</td><td colspan="11">void *, SubSystemData</td><td>0x0028</td></tr>
<tr><td>0x0018</td><td colspan="11">void *, ProcessHeap</td><td>0x0030</td></tr>
<tr><td>0x001C</td><td colspan="11">struct _RTL_CRITICAL_SECTION *, FastPebLock</td><td>0x0038</td></tr>
<tr><td>0x0020</td><td colspan="2">void *, FastPebLockRoutine</td><td>void *, SparePtr1</td><td colspan="8">void *, AtlThunkSListPtr</td><td>0x0040</td></tr>
<tr><td>0x0024</td><td colspan="2">void *, FastPebUnlockRoutine</td><td colspan="2">void *, SparePtr2</td><td colspan="7">void *, IFEOKey</td><td>0x0048</td></tr>
<tr><td>0x0028</td><td colspan="4" rowspan="7">unsigned long, EnvironmentUpdateCount</td><td colspan="7">unsigned long, CrossProcessFlags</td><td>0x0050</td></tr>
<tr><td>0x0028:0x00(1)</td><td colspan="7">unsigned long, ProcessInJob</td><td>0x0050:0x00(1)</td></tr>
<tr><td>0x0028:0x01(1)</td><td colspan="7">unsigned long, ProcessInitializing</td><td>0x0050:0x01(1)</td></tr>
<tr><td>0x0028:0x02(1)</td><td rowspan="4">unsigned long, ReservedBits0</td><td colspan="6">unsigned long, ProcessUsingVEH</td><td>0x0050:0x02(1)</td></tr>
<tr><td>0x0028:0x03(1)</td><td colspan="6">unsigned long, ProcessUsingVCH</td><td>0x0050:0x03(1)</td></tr>
<tr><td>0x0028:0x04(1C)</td><td rowspan="2">unsigned long, ReservedBits0</td><td colspan="5">unsigned long, ProcessUsingFTH</td><td>0x0050:0x04(1C)</td></tr>
<tr><td>0x0028:0x05(1B)</td><td colspan="5">unsigned long, ReservedBits0</td><td>0x0050:0x05(1B)</td></tr>
<tr><td>0x002C</td><td colspan="4">void *, KernelCallbackTable</td><td colspan="7">void *, KernelCallbackTable / void *, UserSharedInfoPtr</td><td>0x0058</td></tr>
<tr><td>0x0030</td><td colspan="11">unsigned long[0x1], SystemReserved</td><td>0x0060</td></tr>
<tr><td>0x0034</td><td rowspan="3">unsigned long, ExecuteOptions</td><td rowspan="4">unsigned long, AtlThunkSListPtr32</td><td rowspan="3">unsigned long, ExecuteOptions</td><td colspan="3" rowspan="4">unsigned long, SpareUlong</td><td>unsigned long, TracingFlags</td><td colspan="4" rowspan="4">unsigned long, AtlThunkSListPtr32</td><td>0x0064</td></tr>
<tr><td>0x0034:0x00(1)</td><td>unsigned long, HeapTracingEnabled</td><td>0x0064:0x00(1)</td></tr>
<tr><td>0x0034:0x00(1)</td><td>unsigned long, CritSecTracingEnabled</td><td>0x0064:0x00(1)</td></tr>
<tr><td>0x0034:0x02(1E)</td><td>unsigned long, SpareBits</td><td>unsigned long, SpareBits</td><td>unsigned long, SpareTracingBits</td><td>0x0064:0x02(1E)</td></tr>
<tr><td>0x0038</td><td colspan="5">struct _PEB_FREE_BLOCK *, FreeList</td><td>unsigned long (x64: unsigned __int64), SparePebPtr0</td><td colspan="5">void *, ApiSetMap</td><td>0x0068</td></tr>
<tr><td>0x003C</td><td colspan="11">unsigned long, TlsExpansionCounter</td><td>0x0070</td></tr>
<tr><td>0x0040</td><td colspan="11">void *, TlsBitmap</td><td>0x0078</td></tr>
<tr><td>0x0044</td><td colspan="11">unsigned long[0x2], TlsBitmapBits</td><td>0x0080</td></tr>
<tr><td>0x004C</td><td colspan="11">void *, ReadOnlySharedMemoryBase</td><td>0x0088</td></tr>
<tr><td>0x0050</td><td colspan="4">void *, ReadOnlySharedMemoryHeap</td><td colspan="7">void *, HotpatchInformation</td><td>0x0090</td></tr>
<tr><td>0x0054</td><td colspan="11">void * *, ReadOnlyStaticServerData</td><td>0x0098</td></tr>
<tr><td>0x0058</td><td colspan="11">void *, AnsiCodePageData</td><td>0x00A0</td></tr>
<tr><td>0x005C</td><td colspan="11">void *, OemCodePageData</td><td>0x00A8</td></tr>
<tr><td>0x0060</td><td colspan="11">void *, UnicodeCaseTableData</td><td>0x00B0</td></tr>
<tr><td>0x0064</td><td colspan="11">unsigned long, NumberOfProcessors</td><td>0x00B8</td></tr>
<tr><td>0x0068</td><td colspan="11">unsigned long, NtGlobalFlag</td><td>0x00BC</td></tr>
<tr><td>0x0070</td><td colspan="11">union _LARGE_INTEGER, CriticalSectionTimeout</td><td>0x00C0</td></tr>
<tr><td>0x0078</td><td colspan="11">unsigned long (x64: unsigned __int64), HeapSegmentReserve</td><td>0x00C8</td></tr>
<tr><td>0x007C</td><td colspan="11">unsigned long (x64: unsigned __int64), HeapSegmentCommit</td><td>0x00D0</td></tr>
<tr><td>0x0080</td><td colspan="11">unsigned long (x64: unsigned __int64), HeapDeCommitTotalFreeThreshold</td><td>0x00D8</td></tr>
<tr><td>0x0084</td><td colspan="11">unsigned long (x64: unsigned __int64), HeapDeCommitFreeBlockThreshold</td><td>0x00E0</td></tr>
<tr><td>0x0088</td><td colspan="11">unsigned long, NumberOfHeaps</td><td>0x00E8</td></tr>
<tr><td>0x008C</td><td colspan="11">unsigned long, MaximumNumberOfHeaps</td><td>0x00EC</td></tr>
<tr><td>0x0090</td><td colspan="11">void * *, ProcessHeaps</td><td>0x00F0</td></tr>
<tr><td>0x0094</td><td colspan="11">void *, GdiSharedHandleTable</td><td>0x00F8</td></tr>
<tr><td>0x0098</td><td colspan="11">void *, ProcessStarterHelper</td><td>0x0100</td></tr>
<tr><td>0x009C</td><td colspan="11">unsigned long, GdiDCAttributeList</td><td>0x0108</td></tr>
<tr><td>0x00A0</td><td colspan="2">void *, LoaderLock</td><td colspan="9">struct _RTL_CRITICAL_SECTION *, LoaderLock</td><td>0x0110</td></tr>
<tr><td>0x00A4</td><td colspan="11">unsigned long, OSMajorVersion</td><td>0x0118</td></tr>
<tr><td>0x00A8</td><td colspan="11">unsigned long, OSMinorVersion</td><td>0x011C</td></tr>
<tr><td>0x00AC</td><td colspan="11">unsigned short, OSBuildNumber</td><td>0x0120</td></tr>
<tr><td>0x00AE</td><td colspan="11">unsigned short, OSCSDVersion</td><td>0x0122</td></tr>
<tr><td>0x00B0</td><td colspan="11">unsigned long, OSPlatformId</td><td>0x0124</td></tr>
<tr><td>0x00B4</td><td colspan="11">unsigned long, ImageSubsystem</td><td>0x0128</td></tr>
<tr><td>0x00B8</td><td colspan="11">unsigned long, ImageSubsystemMajorVersion</td><td>0x012C</td></tr>
<tr><td>0x00BC</td><td colspan="11">unsigned long, ImageSubsystemMinorVersion</td><td>0x0130</td></tr>
<tr><td>0x00C0</td><td colspan="5">unsigned long (x64: unsigned __int64), ImageProcessAffinityMask</td><td colspan="6">unsigned long (x64: unsigned __int64), ActiveProcessAffinityMask</td><td>0x0138</td></tr>
<tr><td>0x00C4</td><td colspan="11">unsigned long[0x22] (x64: unsigned long[0x3C]), GdiHandleBuffer</td><td>0x0140</td></tr>
<tr><td>0x014C</td><td colspan="11">function *, PostProcessInitRoutine</td><td>0x0230</td></tr>
<tr><td>0x0150</td><td colspan="11">void *, TlsExpansionBitmap</td><td>0x0238</td></tr>
<tr><td>0x0154</td><td colspan="11">unsigned long[0x20], TlsExpansionBitmapBits</td><td>0x0240</td></tr>
<tr><td>0x01D4</td><td colspan="11">unsigned long, SessionId</td><td>0x02C0</td></tr>
<tr><td>0x01D8</td><td colspan="11">union _ULARGE_INTEGER, AppCompatFlags</td><td>0x02C8</td></tr>
<tr><td>0x01E0</td><td colspan="11">union _ULARGE_INTEGER, AppCompatFlagsUser</td><td>0x02D0</td></tr>
<tr><td>0x01E8</td><td colspan="11">void *, pShimData</td><td>0x02D8</td></tr>
<tr><td>0x01EC</td><td colspan="11">void *, AppCompatInfo</td><td>0x02E0</td></tr>
<tr><td>0x01F0</td><td colspan="11">struct _UNICODE_STRING, CSDVersion</td><td>0x02E8</td></tr>
<tr><td>0x01F8</td><td colspan="2">void *, ActivationContextData</td><td colspan="9">const struct _ACTIVATION_CONTEXT_DATA *, ActivationContextData</td><td>0x02F8</td></tr>
<tr><td>0x01FC</td><td colspan="2">void *, ProcessAssemblyStorageMap</td><td colspan="9">struct _ASSEMBLY_STORAGE_MAP *, ProcessAssemblyStorageMap</td><td>0x0300</td></tr>
<tr><td>0x0200</td><td colspan="2">void *, SystemDefaultActivationContextData</td><td colspan="9">const struct _ACTIVATION_CONTEXT_DATA *, SystemDefaultActivationContextData</td><td>0x0308</td></tr>
<tr><td>0x0204</td><td colspan="2">void *, SystemAssemblyStorageMap</td><td colspan="9">struct _ASSEMBLY_STORAGE_MAP *, SystemAssemblyStorageMap</td><td>0x0310</td></tr>
<tr><td>0x0208</td><td colspan="11">unsigned long (x64: unsigned __int64), MinimumStackCommit</td><td>0x0318</td></tr>
<tr><td>0x020C</td><td></td><td></td><td colspan="2">void * *, FlsCallback</td><td colspan="7">struct _FLS_CALLBACK_INFO *, FlsCallback</td><td>0x0320</td></tr>
<tr><td>0x0210</td><td></td><td></td><td colspan="9">struct _LIST_ENTRY, FlsListHead</td><td>0x0328</td></tr>
<tr><td>0x0218</td><td></td><td></td><td colspan="9">void *, FlsBitmap</td><td>0x0338</td></tr>
<tr><td>0x021C</td><td></td><td></td><td colspan="9">unsigned long[0x4], FlsBitmapBits</td><td>0x0340</td></tr>
<tr><td>0x022C</td><td></td><td></td><td colspan="9">unsigned long, FlsHighIndex</td><td>0x0350</td></tr>
<tr><td>0x0230</td><td></td><td></td><td></td><td></td><td colspan="7">void *, WerRegistrationData</td><td>0x0358</td></tr>
<tr><td>0x0234</td><td></td><td></td><td></td><td></td><td colspan="7">void *, WerShipAssertPtr</td><td>0x0360</td></tr>
<tr><td>0x0238</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">void *, pContextData</td><td colspan="3">void *, pUnused</td><td>0x0368</td></tr>
<tr><td>0x023C</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="5">void *, pImageHeaderHash</td><td>0x0370</td></tr>
<tr><td>0x0240</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">unsigned long, TracingFlags</td><td>0x0378</td></tr>
<tr><td>0x0240:0x00(1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">unsigned long, HeapTracingEnabled</td><td>0x0378:0x00(1)</td></tr>
<tr><td>0x0240:0x01(1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">unsigned long, CritSecTracingEnabled</td><td>0x0378:0x01(1)</td></tr>
<tr><td>0x0240:0x02(1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td rowspan="2">unsigned long, SpareTracingBits</td><td colspan="3">unsigned long, LibLoaderTracingEnabled</td><td>0x0378:0x02(1)</td></tr>
<tr><td>0x0240:0x03(1D)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="3">unsigned long, SpareTracingBits</td><td>0x0378:0x03(1D)</td></tr>
<tr><td>0x0248</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="3">unsigned __int64, CsrServerReadOnlySharedMemoryBase</td><td>0x0380</td></tr>
<tr><td></td><td>XP, XP SP1</td><td>XP SP2, XP SP3</td><td>2003</td><td>2003 SP1, 2003 SP2</td><td>Vista</td><td>Vista SP1, Vista SP2</td><td>Win7 Beta</td><td>Win7 RC, Win7 RTM</td><td>Win8 Dev Prev x64 (8102)</td><td>Win8 Beta</td><td>Win8 RC, Win8 RTM</td><td></td></tr>
</table>