PEB

进程环境块，描述线程的状态

https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb

在windbg_x86调试器下查看`PEB`如下

```
0:000> dt _PEB
ntdll!_PEB
   +0x000 InheritedAddressSpace : UChar
   +0x001 ReadImageFileExecOptions : UChar
   +0x002 BeingDebugged    : UChar
   +0x003 BitField         : UChar
   +0x003 ImageUsesLargePages : Pos 0, 1 Bit
   +0x003 IsProtectedProcess : Pos 1, 1 Bit
   +0x003 IsImageDynamicallyRelocated : Pos 2, 1 Bit
   +0x003 SkipPatchingUser32Forwarders : Pos 3, 1 Bit
   +0x003 IsPackagedProcess : Pos 4, 1 Bit
   +0x003 IsAppContainer   : Pos 5, 1 Bit
   +0x003 IsProtectedProcessLight : Pos 6, 1 Bit
   +0x003 IsLongPathAwareProcess : Pos 7, 1 Bit
   +0x004 Mutant           : Ptr32 Void
   +0x008 ImageBaseAddress : Ptr32 Void
   +0x00c Ldr              : Ptr32 _PEB_LDR_DATA
   +0x010 ProcessParameters : Ptr32 _RTL_USER_PROCESS_PARAMETERS
   +0x014 SubSystemData    : Ptr32 Void
   +0x018 ProcessHeap      : Ptr32 Void
   +0x01c FastPebLock      : Ptr32 _RTL_CRITICAL_SECTION
   +0x020 AtlThunkSListPtr : Ptr32 _SLIST_HEADER
   +0x024 IFEOKey          : Ptr32 Void
   +0x028 CrossProcessFlags : Uint4B
   +0x028 ProcessInJob     : Pos 0, 1 Bit
   +0x028 ProcessInitializing : Pos 1, 1 Bit
   +0x028 ProcessUsingVEH  : Pos 2, 1 Bit
   +0x028 ProcessUsingVCH  : Pos 3, 1 Bit
   +0x028 ProcessUsingFTH  : Pos 4, 1 Bit
   +0x028 ProcessPreviouslyThrottled : Pos 5, 1 Bit
   +0x028 ProcessCurrentlyThrottled : Pos 6, 1 Bit
   +0x028 ProcessImagesHotPatched : Pos 7, 1 Bit
   +0x028 ReservedBits0    : Pos 8, 24 Bits
   +0x02c KernelCallbackTable : Ptr32 Void
   +0x02c UserSharedInfoPtr : Ptr32 Void
   +0x030 SystemReserved   : Uint4B
   +0x034 AtlThunkSListPtr32 : Ptr32 _SLIST_HEADER
   +0x038 ApiSetMap        : Ptr32 Void
   +0x03c TlsExpansionCounter : Uint4B
   +0x040 TlsBitmap        : Ptr32 Void
   +0x044 TlsBitmapBits    : [2] Uint4B
   +0x04c ReadOnlySharedMemoryBase : Ptr32 Void
   +0x050 SharedData       : Ptr32 Void
   +0x054 ReadOnlyStaticServerData : Ptr32 Ptr32 Void
   +0x058 AnsiCodePageData : Ptr32 Void
   +0x05c OemCodePageData  : Ptr32 Void
   +0x060 UnicodeCaseTableData : Ptr32 Void
   +0x064 NumberOfProcessors : Uint4B
   +0x068 NtGlobalFlag     : Uint4B
   +0x070 CriticalSectionTimeout : _LARGE_INTEGER
   +0x078 HeapSegmentReserve : Uint4B
   +0x07c HeapSegmentCommit : Uint4B
   +0x080 HeapDeCommitTotalFreeThreshold : Uint4B
   +0x084 HeapDeCommitFreeBlockThreshold : Uint4B
   +0x088 NumberOfHeaps    : Uint4B
   +0x08c MaximumNumberOfHeaps : Uint4B
   +0x090 ProcessHeaps     : Ptr32 Ptr32 Void
   +0x094 GdiSharedHandleTable : Ptr32 Void
   +0x098 ProcessStarterHelper : Ptr32 Void
   +0x09c GdiDCAttributeList : Uint4B
   +0x0a0 LoaderLock       : Ptr32 _RTL_CRITICAL_SECTION
   +0x0a4 OSMajorVersion   : Uint4B
   +0x0a8 OSMinorVersion   : Uint4B
   +0x0ac OSBuildNumber    : Uint2B
   +0x0ae OSCSDVersion     : Uint2B
   +0x0b0 OSPlatformId     : Uint4B
   +0x0b4 ImageSubsystem   : Uint4B
   +0x0b8 ImageSubsystemMajorVersion : Uint4B
   +0x0bc ImageSubsystemMinorVersion : Uint4B
   +0x0c0 ActiveProcessAffinityMask : Uint4B
   +0x0c4 GdiHandleBuffer  : [34] Uint4B
   +0x14c PostProcessInitRoutine : Ptr32     void
   +0x150 TlsExpansionBitmap : Ptr32 Void
   +0x154 TlsExpansionBitmapBits : [32] Uint4B
   +0x1d4 SessionId        : Uint4B
   +0x1d8 AppCompatFlags   : _ULARGE_INTEGER
   +0x1e0 AppCompatFlagsUser : _ULARGE_INTEGER
   +0x1e8 pShimData        : Ptr32 Void
   +0x1ec AppCompatInfo    : Ptr32 Void
   +0x1f0 CSDVersion       : _UNICODE_STRING
   +0x1f8 ActivationContextData : Ptr32 _ACTIVATION_CONTEXT_DATA
   +0x1fc ProcessAssemblyStorageMap : Ptr32 _ASSEMBLY_STORAGE_MAP
   +0x200 SystemDefaultActivationContextData : Ptr32 _ACTIVATION_CONTEXT_DATA
   +0x204 SystemAssemblyStorageMap : Ptr32 _ASSEMBLY_STORAGE_MAP
   +0x208 MinimumStackCommit : Uint4B
   +0x20c SparePointers    : [4] Ptr32 Void
   +0x21c SpareUlongs      : [5] Uint4B
   +0x230 WerRegistrationData : Ptr32 Void
   +0x234 WerShipAssertPtr : Ptr32 Void
   +0x238 pUnused          : Ptr32 Void
   +0x23c pImageHeaderHash : Ptr32 Void
   +0x240 TracingFlags     : Uint4B
   +0x240 HeapTracingEnabled : Pos 0, 1 Bit
   +0x240 CritSecTracingEnabled : Pos 1, 1 Bit
   +0x240 LibLoaderTracingEnabled : Pos 2, 1 Bit
   +0x240 SpareTracingBits : Pos 3, 29 Bits
   +0x248 CsrServerReadOnlySharedMemoryBase : Uint8B
   +0x250 TppWorkerpListLock : Uint4B
   +0x254 TppWorkerpList   : _LIST_ENTRY
   +0x25c WaitOnAddressHashTable : [128] Ptr32 Void
   +0x45c TelemetryCoverageHeader : Ptr32 Void
   +0x460 CloudFileFlags   : Uint4B
   +0x464 CloudFileDiagFlags : Uint4B
   +0x468 PlaceholderCompatibilityMode : Char
   +0x469 PlaceholderCompatibilityModeReserved : [7] Char
   +0x470 LeapSecondData   : Ptr32 _LEAP_SECOND_DATA
   +0x474 LeapSecondFlags  : Uint4B
   +0x474 SixtySecondEnabled : Pos 0, 1 Bit
   +0x474 Reserved         : Pos 1, 31 Bits
   +0x478 NtGlobalFlag2    : Uint4B
```

TEB

线程环境块，描述线程的状态

https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-teb

在windbg_x86调试器下查看`TEB`如下

```
0:000> dt _TEB
ntdll!_TEB
   +0x000 NtTib            : _NT_TIB    // TIB
   +0x01c EnvironmentPointer : Ptr32 Void
   +0x020 ClientId         : _CLIENT_ID
   +0x028 ActiveRpcHandle  : Ptr32 Void
   +0x02c ThreadLocalStoragePointer : Ptr32 Void    // 指向TLS的指针数组
   +0x030 ProcessEnvironmentBlock : Ptr32 _PEB  // 指向PEB，TEB与PEB是n：1
   +0x034 LastErrorValue   : Uint4B
   +0x038 CountOfOwnedCriticalSections : Uint4B
   +0x03c CsrClientThread  : Ptr32 Void
   +0x040 Win32ThreadInfo  : Ptr32 Void
   +0x044 User32Reserved   : [26] Uint4B
   +0x0ac UserReserved     : [5] Uint4B
   +0x0c0 WOW32Reserved    : Ptr32 Void
   +0x0c4 CurrentLocale    : Uint4B
   +0x0c8 FpSoftwareStatusRegister : Uint4B
   +0x0cc ReservedForDebuggerInstrumentation : [16] Ptr32 Void
   +0x10c SystemReserved1  : [26] Ptr32 Void
   +0x174 PlaceholderCompatibilityMode : Char
   +0x175 PlaceholderHydrationAlwaysExplicit : UChar
   +0x176 PlaceholderReserved : [10] Char
   +0x180 ProxiedProcessId : Uint4B
   +0x184 _ActivationStack : _ACTIVATION_CONTEXT_STACK
   +0x19c WorkingOnBehalfTicket : [8] UChar
   +0x1a4 ExceptionCode    : Int4B
   +0x1a8 ActivationContextStackPointer : Ptr32 _ACTIVATION_CONTEXT_STACK
   +0x1ac InstrumentationCallbackSp : Uint4B
   +0x1b0 InstrumentationCallbackPreviousPc : Uint4B
   +0x1b4 InstrumentationCallbackPreviousSp : Uint4B
   +0x1b8 InstrumentationCallbackDisabled : UChar
   +0x1b9 SpareBytes       : [23] UChar
   +0x1d0 TxFsContext      : Uint4B
   +0x1d4 GdiTebBatch      : _GDI_TEB_BATCH
   +0x6b4 RealClientId     : _CLIENT_ID
   +0x6bc GdiCachedProcessHandle : Ptr32 Void
   +0x6c0 GdiClientPID     : Uint4B
   +0x6c4 GdiClientTID     : Uint4B
   +0x6c8 GdiThreadLocalInfo : Ptr32 Void
   +0x6cc Win32ClientInfo  : [62] Uint4B
   +0x7c4 glDispatchTable  : [233] Ptr32 Void
   +0xb68 glReserved1      : [29] Uint4B
   +0xbdc glReserved2      : Ptr32 Void
   +0xbe0 glSectionInfo    : Ptr32 Void
   +0xbe4 glSection        : Ptr32 Void
   +0xbe8 glTable          : Ptr32 Void
   +0xbec glCurrentRC      : Ptr32 Void
   +0xbf0 glContext        : Ptr32 Void
   +0xbf4 LastStatusValue  : Uint4B
   +0xbf8 StaticUnicodeString : _UNICODE_STRING
   +0xc00 StaticUnicodeBuffer : [261] Wchar
   +0xe0c DeallocationStack : Ptr32 Void
   +0xe10 TlsSlots         : [64] Ptr32 Void    // 线程局部存储所使用的数组
   +0xf10 TlsLinks         : _LIST_ENTRY
   +0xf18 Vdm              : Ptr32 Void
   +0xf1c ReservedForNtRpc : Ptr32 Void
   +0xf20 DbgSsReserved    : [2] Ptr32 Void
   +0xf28 HardErrorMode    : Uint4B
   +0xf2c Instrumentation  : [9] Ptr32 Void
   +0xf50 ActivityId       : _GUID
   +0xf60 SubProcessTag    : Ptr32 Void
   +0xf64 PerflibData      : Ptr32 Void
   +0xf68 EtwTraceData     : Ptr32 Void
   +0xf6c WinSockData      : Ptr32 Void
   +0xf70 GdiBatchCount    : Uint4B
   +0xf74 CurrentIdealProcessor : _PROCESSOR_NUMBER
   +0xf74 IdealProcessorValue : Uint4B
   +0xf74 ReservedPad0     : UChar
   +0xf75 ReservedPad1     : UChar
   +0xf76 ReservedPad2     : UChar
   +0xf77 IdealProcessor   : UChar
   +0xf78 GuaranteedStackBytes : Uint4B
   +0xf7c ReservedForPerf  : Ptr32 Void
   +0xf80 ReservedForOle   : Ptr32 Void
   +0xf84 WaitingOnLoaderLock : Uint4B
   +0xf88 SavedPriorityState : Ptr32 Void
   +0xf8c ReservedForCodeCoverage : Uint4B
   +0xf90 ThreadPoolData   : Ptr32 Void
   +0xf94 TlsExpansionSlots : Ptr32 Ptr32 Void
   +0xf98 MuiGeneration    : Uint4B
   +0xf9c IsImpersonating  : Uint4B
   +0xfa0 NlsCache         : Ptr32 Void
   +0xfa4 pShimData        : Ptr32 Void
   +0xfa8 HeapData         : Uint4B
   +0xfac CurrentTransactionHandle : Ptr32 Void
   +0xfb0 ActiveFrame      : Ptr32 _TEB_ACTIVE_FRAME
   +0xfb4 FlsData          : Ptr32 Void
   +0xfb8 PreferredLanguages : Ptr32 Void
   +0xfbc UserPrefLanguages : Ptr32 Void
   +0xfc0 MergedPrefLanguages : Ptr32 Void
   +0xfc4 MuiImpersonation : Uint4B
   +0xfc8 CrossTebFlags    : Uint2B
   +0xfc8 SpareCrossTebBits : Pos 0, 16 Bits
   +0xfca SameTebFlags     : Uint2B
   +0xfca SafeThunkCall    : Pos 0, 1 Bit
   +0xfca InDebugPrint     : Pos 1, 1 Bit
   +0xfca HasFiberData     : Pos 2, 1 Bit
   +0xfca SkipThreadAttach : Pos 3, 1 Bit
   +0xfca WerInShipAssertCode : Pos 4, 1 Bit
   +0xfca RanProcessInit   : Pos 5, 1 Bit
   +0xfca ClonedThread     : Pos 6, 1 Bit
   +0xfca SuppressDebugMsg : Pos 7, 1 Bit
   +0xfca DisableUserStackWalk : Pos 8, 1 Bit
   +0xfca RtlExceptionAttached : Pos 9, 1 Bit
   +0xfca InitialThread    : Pos 10, 1 Bit
   +0xfca SessionAware     : Pos 11, 1 Bit
   +0xfca LoadOwner        : Pos 12, 1 Bit
   +0xfca LoaderWorker     : Pos 13, 1 Bit
   +0xfca SkipLoaderInit   : Pos 14, 1 Bit
   +0xfca SpareSameTebBits : Pos 15, 1 Bit
   +0xfcc TxnScopeEnterCallback : Ptr32 Void
   +0xfd0 TxnScopeExitCallback : Ptr32 Void
   +0xfd4 TxnScopeContext  : Ptr32 Void
   +0xfd8 LockCount        : Uint4B
   +0xfdc WowTebOffset     : Int4B
   +0xfe0 ResourceRetValue : Ptr32 Void
   +0xfe4 ReservedForWdf   : Ptr32 Void
   +0xfe8 ReservedForCrt   : Uint8B
   +0xff0 EffectiveContainerId : _GUID
```

TIB

```
ntdll!_NT_TIB
   +0x000 ExceptionList    : Ptr32 _EXCEPTION_REGISTRATION_RECORD   // 异常链表
   +0x004 StackBase        : Ptr32 Void
   +0x008 StackLimit       : Ptr32 Void
   +0x00c SubSystemTib     : Ptr32 Void
   +0x010 FiberData        : Ptr32 Void
   +0x010 Version          : Uint4B
   +0x014 ArbitraryUserPointer : Ptr32 Void
   +0x018 Self             : Ptr32 _NT_TIB  // 回指自身
```