**如何获得其他进程的PEB结构体信息。**

**NTSTATUS WINAPI NtQueryInformationProcess(**

**\_\_in HANDLE ProcessHandle,//进程句柄**

**\_\_in PROCESSINFOCLASS ProcessInformationClass,//** ProcessBasicInformation

**\_\_out PVOID ProcessInformation,//** PROCESS\_BASIC\_INFORMATION

**\_\_in ULONG ProcessInformationLength,//前边结构体的大小**

**\_\_out\_opt PULONG ReturnLength//返回值的大小。**

**);**

typedef struct \_PEB {

BYTE Reserved1[2];

BYTE BeingDebugged;

BYTE Reserved2[1];

PVOID Reserved3[2];

PPEB\_LDR\_DATA Ldr;

PRTL\_USER\_PROCESS\_PARAMETERS ProcessParameters;

BYTE Reserved4[104];

PVOID Reserved5[52];

PPS\_POST\_PROCESS\_INIT\_ROUTINE PostProcessInitRoutine;

BYTE Reserved6[128];

PVOID Reserved7[1];

ULONG SessionId;

} PEB, \*PPEB;

typedef struct \_RTL\_USER\_PROCESS\_PARAMETERS {

BYTE Reserved1[16];

PVOID Reserved2[10];

UNICODE\_STRING ImagePathName;

UNICODE\_STRING CommandLine;

} RTL\_USER\_PROCESS\_PARAMETERS, \*PRTL\_USER\_PROCESS\_PARAMETERS;

typedef struct \_UNICODE\_STRING {

USHORT Length;

USHORT MaximumLength;

PWSTR Buffer;

} UNICODE\_STRING;

**获取进程中的堆和堆内存分配情况。**