目录

[如何查看某映像(sys exe dll)的版本号、时间、公司等信息？ 2](#_Toc434532266)

[如何列出以T开头的模块以查看他们的基址？ 3](#_Toc434532267)

[如何列出所有进程EPROCESS地址？ 3](#_Toc434532268)

[如何按ImageName给模块排序 4](#_Toc434532269)

[如何通过 指定PEPROCESS、进程映像名、进程ID 获取进程信息 4](#_Toc434532270)

[如何在内核态调试中下用户态进程断点？ 4](#_Toc434532271)

[如何根据 基址、名称获取对象信息？ 5](#_Toc434532272)

[如何根据句柄获取对象信息？ 5](#_Toc434532273)

[如何在物理地址下断？ 5](#_Toc434532274)

[如何获取Fs:[0]所在地址？ 5](#_Toc434532275)

[如何获取某结构体大小？ 5](#_Toc434532276)

[如何下删除断点？ 5](#_Toc434532277)

### 如何查看某映像(sys exe dll)的版本号、时间、公司等信息？

kd> lmvm nt\*

start end module name

7c920000 7c9b3000 ntdll (pdb symbols) d:\symcachel\ntdll.pdb\1751003260CA42598C0FB326585000ED2\ntdll.pdb

Loaded symbol image file: ntdll.dll

Mapped memory image file: d:\symcachel\ntdll.dll\4802BDC593000\ntdll.dll

Image path: ntdll.dll

Image name: ntdll.dll

Timestamp: Mon Apr 14 10:13:25 2008 (4802BDC5)

CheckSum: 00097CB7

ImageSize: 00093000

Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4

804d8000 806d0480 nt (pdb symbols) d:\symcachel\ntkrnlpa.pdb\30B5FB31AE7E4ACAABA750AA241FF3311\ntkrnlpa.pdb

Loaded symbol image file: ntkrnlpa.exe

Image path: ntkrnlpa.exe

Image name: ntkrnlpa.exe

Timestamp: Mon Apr 14 02:31:06 2008 (4802516A)

CheckSum: 002050D3

ImageSize: 001F8480

File version: 5.1.2600.5512

Product version: 5.1.2600.5512

File flags: 0 (Mask 3F)

File OS: 40004 NT Win32

File type: 1.0 App

File date: 00000000.00000000

Translations: 0804.04b0

CompanyName: Microsoft Corporation

ProductName: Microsoft(R) Windows(R) Operating System

InternalName: ntkrnlpa.exe

OriginalFilename: ntkrnlpa.exe

ProductVersion: 5.1.2600.5512

FileVersion: 5.1.2600.5512 (xpsp.080413-2111)

FileDescription: NT Kernel & System

LegalCopyright: (C) Microsoft Corporation. All rights reserved.

f8398000 f8424600 Ntfs (deferred)

Image path: Ntfs.sys

Image name: Ntfs.sys

Timestamp: Mon Apr 14 03:15:49 2008 (48025BE5)

CheckSum: 0009586B

ImageSize: 0008C600

Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4

### 如何列出以T开头的模块以查看他们的基址？

kd> lm m T\*

start end module name

b1d28000 b1d4d000 TAOKernelXP (deferred)

b1d75000 b1d8ec80 TAOAccelerator (deferred)

b2ce8000 b2d0a700 TFsFlt (deferred)

b2d0b000 b2d33580 TSDefenseBt (deferred)

b2d34000 b2d65160 TSKsp (deferred)

b2d8c000 b2da2980 TSSysKit (deferred)

b2e3c000 b2e94380 tcpip (deferred)

f8515000 f8531c00 TsFltMgr (deferred)

f889a000 f88a3f00 termdd (pdb symbols) d:\symcachel\termdd.pdb\C04E4855F20641ECB654BB1AD575B8611\termdd.pdb

f8992000 f8996a80 TDI (pdb symbols) d:\symcachel\tdi.pdb\545742C029D24374BD687966638629EB1\tdi.pdb

f8a6a000 f8a6f380 TS888 (deferred)

f8a8a000 f8a8f500 TDTCP (deferred)

### 如何列出所有进程EPROCESS地址？

dml\_proc 或 !process

kd> !dml\_proc

Address PID Image file name

821b9660 4 System

81c1cca8 2c0 smss.exe

81c3d660 2e0 autochk.exe

81cde760 304 csrss.exe

81f5c758 324 winlogon.exe

81f16628 350 services.exe

81dfdc08 360 lsass.exe

8200f020 444 vmacthlp.exe

81d7eda0 454 svchost.exe

81c46890 490 BaiduHips.exe

81f0eda0 4b0 BaiduSdSvc.exe

81e7e410 500 QQPXRTP.exe

81f5f638 510 logonui.exe

81f253c0 5f4 svchost.exe

81b73890 648 svchost.exe

81dff898 6dc svchost.exe

81e27020 780 userinit.exe

81bf7578 7f4 svchost.exe

81d2a020 f0 ZhuDongFangYu.e

81b78da0 148 explorer.exe

81394890 2e4 spoolsv.exe

### 如何按ImageName给模块排序

kd> lmDksm

start end module name

b2ae3000 b2b05000 360AntiHacker (deferred)

b2a21000 b2a38000 360boost (deferred)

b2f44000 b2f7a000 360Box (deferred)

b2e95000 b2ee6700 360netmon (deferred)

b2a38000 b2a6d000 360qpesv (deferred)

f8211000 f821d000 360reskit (deferred)

b2f1a000 b2f43900 360SelfProtection (deferred)

f84e7000 f8514500 ACPI (deferred)

b2dca000 b2debb80 afd (deferred)

f870a000 f8714580 agp440 (deferred)

f8466000 f847d900 atapi (deferred)

f8d21000 f8d21c00 audstub (pdb symbols) d:\symcachel\audstub.pdb\6B3BF8F0C8834E7E8EFE53B7A91E2A3F1\audstub.pdb

b2a6d000 b2a9a000 BAPIDRV (deferred)

f8ab2000 f8ab5f00 BATTC (deferred)

### 如何通过 指定PEPROCESS、进程映像名、进程ID 获取进程信息

### 如何在内核态调试中下用户态进程断点？

1. !process 0 0

### 如何根据 基址、名称获取对象信息？

### 如何根据句柄获取对象信息？

### 如何在物理地址下断？

### 如何获取Fs:[0]所在地址？

### 如何获取某结构体大小？

### 如何下删除断点？