```
;-------------------------------------------------------------------------
;
;       Disassembly listing generated by PE Explorer version 1.99
;       Heaventools Software (http://www.heaventools.com)
;
;-------------------------------------------------------------------------
; Name: .text (Code Section)
; Virtual Address:   000102C0h  Virtual Size:    00000BA8h
; Pointer To RawData: 000002C0h  Size Of RawData: 00000BC0h
;
L000102C0:
                test    dword ptr [esp+04h],00020000h
                jz      L000102D1
                db      2Eh;   '.'
                jmp     [L00011198]
L000102D1:
                sub     esp,00000004h
                push    ebp
                mov     ebp,esp
                cli
                pushad
                push    ds
                push    es
                push    gs
                push    fs
                mov     bx,0023h
                mov     ds,bx
                mov     es,bx
                mov     gs,bx
                mov     bx,0030h
                mov     fs,bx
                push    eax
                mov     eax,cr4
                and     eax,000007F7h
                mov     cr4,eax
                mov     eax,00000400h
                mov     dr7,eax
                pop     eax
                call    SUB_L0001038E
                mov     eax,cs:[L00011118]
                cmp     eax,00000000h
                jz      L0001031A
                jmp     L00010339
L0001031A:
                pushfd
                xor     eax,eax
                mov     ax,cs
                push    eax
                push    L0001032D
```

```
                jmp     cs:[L00011198]
L0001032D:
                db      0Fh;
                db      A1h;   'ö'
                db      0Fh;
                db      A9h;   'c'
                db      07h;
                db      1Fh;
                db      61h;   'a'
                db      5Dh;   ']'
                db      83h;   '?'
                db      C4h;   ',,'
                db      04h;
                db      CFh;   '□
L00010339:
                mov     ebx,cs:[L00010F64]
                cmp     ebx,00000031h
                jnz     L0001034B
                mov     al,20h
                out     20h,al
                jmp     L0001036B
L0001034B:
                push    ebx
                sub     esp,00000004h
                push    esp
                push    ebx
                mov     eax,00000009h
                push    eax
                call    jmp_HAL.dll!HalBeginSystemInterrupt
                or      eax,eax
                jz      L00010368
                call    jmp_HAL.dll!HalEndSystemInterrupt
                sub     esp,00000008h
L00010368:
                add     esp,00000008h
L0001036B:
                pop     fs
                pop     gs
                pop     es
                pop     ds
                popad
                pop     ebp
                add     esp,00000004h
                iretd



;-------------------------------------------------------------------------------
```

```
SUB_L00010377:
                push    ecx
                xor     ecx,ecx
L0001037A:
                in      al,64h
                test    al,02h
                loopnz  L0001037A
                pop     ecx
                retn
;---------------------------------------------------------------------------
SUB_L00010382:
                push    ecx
                xor     ecx,ecx
L00010385:
                in      al,64h
                test    al,01h
                loopz   L00010385
                pop     ecx
                retn
;---------------------------------------------------------------------------
                Align   2
SUB_L0001038E:
                push    esi
                xor     esi,esi
                cmp     [L0001111C],esi
                mov     [L00011118],esi
                jnz     L000103A7
                mov     [L00011118],esi
                pop     esi
                retn
;---------------------------------------------------------------------------
L000103A7:
                cmp     [L00011130],esi
                jz      L000103BD
                mov     [L00011118],esi
                mov     [L00011130],esi
                pop     esi
                retn
;---------------------------------------------------------------------------
L000103BD:
                call    SUB_L00010382
                in      al,60h
                mov     [L00011141],al
                cmp     [L00011134],esi
                jz      L000103E3
                mov     [L00011134],esi
                mov     dword ptr [L00011118],00000001h
                pop     esi
                retn
```

```
;--------------------------------------------------------------------------
L000103E3:
                movzx eax,[L00011141]
                push  edi
                push  00000001h
                cmp   eax,0000008Dh
                pop   edi
                jg    L000104E4
                cmp   eax,00000082h
                jge   CASE_0001059B_PROC0000
                cmp   eax,00000037h
                jg    L0001047D
                jz    CASE_0001059B_PROC0003
                cmp   eax,00000029h
                jg    L00010455
                cmp   eax,0000001Eh
                jge   CASE_0001059B_PROC0000
                cmp   eax,00000002h
                jl    CASE_0001059B_PROC0004
                cmp   eax,0000000Dh
                jle   CASE_0001059B_PROC0000
                cmp   eax,0000000Fh
                jle   CASE_0001059B_PROC0004
                cmp   eax,0000001Bh
                jle   CASE_0001059B_PROC0000
                cmp   eax,0000001Dh
                jnz   CASE_0001059B_PROC0004
L0001044A:
                mov   [L00011120],edi
                jmp   CASE_0001059B_PROC0004
L00010455:
                cmp   eax,0000002Ah
                jz    L00010472
                jle   CASE_0001059B_PROC0004
                cmp   eax,00000035h
                jle   CASE_0001059B_PROC0000
                cmp   eax,00000036h
                jnz   CASE_0001059B_PROC0004
L00010472:
                mov   [L0001112C],edi
                jmp   CASE_0001059B_PROC0004
L0001047D:
                cmp   eax,0000004Dh
                jg    L000104BD
                cmp   eax,0000004Bh
                jge   CASE_0001059B_PROC0005
                cmp   eax,00000045h
                jz    L000104A8
                cmp   eax,00000046h
```

```
                jle     CASE_0001059B_PROC0004
                cmp     eax,00000049h
                jle     CASE_0001059B_PROC0005
                cmp     eax,0000004Ah
                jz      CASE_0001059B_PROC0000
                jmp     CASE_0001059B_PROC0004
L000104A8:
                xor     eax,eax
                cmp     [L00011128],esi
                setz    al
                mov     [L00011128],eax
                jmp     CASE_0001059B_PROC0004
L000104BD:
                cmp     eax,0000004Eh
                jz      CASE_0001059B_PROC0000
                jle     CASE_0001059B_PROC0004
                cmp     eax,00000053h
                jle     CASE_0001059B_PROC0005
                cmp     eax,0000005Ah
                jle     CASE_0001059B_PROC0004
                cmp     eax,0000005Ch
                jg      CASE_0001059B_PROC0004
                jmp     L0001044A
L000104E4:
                add     eax,FFFFFF70h
                cmp     eax,0000004Ch
                ja      CASE_0001059B_PROC0004
                movzx eax,[eax+CASE_000105B7]
                jmp     [CASE_PROCTABLE_0001059B+eax*4]
CASE_0001059B_PROC0000:
                cmp     [L00011120],esi
                jnz     CASE_0001059B_PROC0004
                jmp     L00010529
CASE_0001059B_PROC0003:
                cmp     [L0001112C],esi
                jnz     CASE_0001059B_PROC0004
                jmp     CASE_0001059B_PROC0000
CASE_0001059B_PROC0001:
                mov     [L00011120],esi
                jmp     CASE_0001059B_PROC0004
CASE_0001059B_PROC0005:
                cmp     [L00011128],esi
                jz      CASE_0001059B_PROC0004
                cmp     byte ptr [L00011140],E0h
                jz      CASE_0001059B_PROC0004
L00010529:
                push    00000001h
                pop     edi
                mov     [L00011118],edi
```

```
                call    SUB_L00010377
                mov     al,EEh
                out     60h,al
                mov     al,[L00011141]
                cmp     al,80h
                jnc     L00010559
                movzx eax,al
                push    esi
                push    esi
                push    L00011160
                mov     [L00011180],eax
                call    [ntoskrnl.exe!KeInsertQueueDpc]
L00010559:
                mov     [L00011134],edi
                jmp     L0001058E
CASE_0001059B_PROC0002:
                mov     [L0001112C],esi
CASE_0001059B_PROC0004:
                mov     [L00011118],esi
                call    SUB_L00010377
                mov     al,D2h
                out     64h,al
                call    SUB_L00010377
                mov     al,[L00011141]
                out     60h,al
                mov     [L00011130],edi
                mov     [L00011118],edi
L0001058E:
                mov     al,[L00011141]
                pop     edi
                mov     [L00011140],al
                pop     esi
                retn
;-----------------------------------------------------------------------------
CASE_PROCTABLE_0001059B: //IOCTL – CASE PROCEDURE TABLE
                dd      CASE_0001059B_PROC0000
                dd      CASE_0001059B_PROC0001
                dd      CASE_0001059B_PROC0002
                dd      CASE_0001059B_PROC0003
                dd      CASE_0001059B_PROC0004
                dd      CASE_0001059B_PROC0005
                dd      CASE_0001059B_PROC0004
CASE_000105B7:
                db      00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 06h, 01h, 00h, 00h
                db      00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 02h, 00h, 00h, 00h, 00h, 00h
                db      00h, 00h, 00h, 00h, 00h, 00h, 02h, 03h, 06h, 06h, 06h, 06h, 06h, 06h, 06h, 06h
                db      06h, 06h, 06h, 06h, 06h, 04h, 06h, 05h, 05h, 05h, 00h, 05h, 05h, 05h, 00h, 05h
                db      05h, 05h, 05h, 05h, 06h, 06h, 06h, 06h, 06h, 06h, 06h, 01h, 01h
SUB_L00010604:
```

```
                mov     eax,[esp+04h]
                xor     edx,edx
                mov     ecx,L00010F70
L0001060F:
                cmp     [ecx],eax
                jz      L00010621
                add     ecx,00000008h
                inc     edx
                cmp     ecx,L00011108
                jl      L0001060F
                jmp     L00010628
L00010621:
                mov     eax,[L00010F74+edx*8]
L00010628:
                retn    0004h
;-----------------------------------------------------------------------------
                Align   4
L0001062C:
                push    ebp
                mov     ebp,esp
                push    ecx
                push    edi
                call    [ntoskrnl.exe!KeQueryTimeIncrement]
                mov     edx,[L000111E8]
                mov     edi,[L000111EC]
                xor     ecx,ecx
                sub     edx,[L00011190]
                push    ecx
                push    eax
                sbb     edi,[L00011194]
                mov     [L000111E0],eax
                mov     [L000111E4],ecx
                push    edi
                push    edx
                call    jmp_ntoskrnl.exe!_allmul
                test    edx,edx
                pop     edi
                jl      L00010693
                jg      L00010673
                cmp     eax,00989680h
                jbe     L00010693
L00010673:
                and     dword ptr [L0001111C],00000000h
                cmp     dword ptr [L00011124],00000001h
                jnz     L00010688
                call    SUB_L00010770
L00010688:
                or      dword ptr [L00011180],FFFFFFFFh
                push    FFFFFFFFh
```

```
                jmp     L000106C8
L00010693:
                mov     eax,[ntoskrnl.exe!KeTickCount]
                mov     [ebp-04h],eax
L0001069B:
                mov     eax,[ebp-04h]
                mov     eax,[eax+04h]
                mov     [L000111EC],eax
                mov     ecx,[ebp-04h]
                mov     ecx,[ecx]
                mov     [L000111E8],ecx
                mov     ecx,[ebp-04h]
                cmp     eax,[ecx+08h]
                jz      L000106BD
                pause                           ; SSE2
                jmp     L0001069B
L000106BD:
                mov     eax,[L00011180]
                cmp     eax,FFFFFFFEh
                jz      L000106CD
                push    eax
L000106C8:
                call    SUB_L00010E1E
L000106CD:
                push    00000000h
                push    00000002h
                push    [L00011188]
                call    [ntoskrnl.exe!KeSetEvent]
                leave
                retn    0010h
;-----------------------------------------------------------------------------
                Align   2
SUB_L000106E2:
                mov     eax,[ntoskrnl.exe!KeNumberProcessors]
                push    ebx
                xor     bl,bl
                push    esi
                cmp     [eax],bl
                jle     L00010741
                mov     esi,L000102C0
                push    edi
                mov     edi,esi
                shr     edi,10h
L000106FA:
                call    jmp_ntoskrnl.exe!KeGetCurrentThread
                push    00000001h
                mov     cl,bl
                pop     edx
                shl     edx,cl
```

```
                push    edx
                push    eax
                call    jmp_ntoskrnl.exe!KeSetAffinityThread
                sidt    [L000111F0]
                mov     eax,[L00010F68]
                mov     eax,[eax+02h]
                cli
                mov     edx,[L00010F60]
                mov     ecx,esi
                mov     [eax+edx*8],cx
                mov     ecx,[L00010F60]
                mov     [eax+ecx*8+06h],di
                sti
                mov     eax,[ntoskrnl.exe!KeNumberProcessors]
                inc     bl
                cmp     bl,[eax]
                jl      L000106FA
                pop     edi
L00010741:
                call    jmp_ntoskrnl.exe!KeGetCurrentThread
                mov     ecx,[ntoskrnl.exe!KeNumberProcessors]
                push    00000001h
                pop     esi
                mov     cl,[ecx]
                mov     edx,esi
                shl     edx,cl
                dec     edx
                push    edx
                push    eax
                call    jmp_ntoskrnl.exe!KeSetAffinityThread
                and     dword ptr [L00011130],00000000h
                mov     [L00011124],esi
                pop     esi
                xor     eax,eax
                pop     ebx
                retn
;------------------------------------------------------------------------------
                Align   4
SUB_L00010770:
                mov     eax,[ntoskrnl.exe!KeNumberProcessors]
                push    ebx
                xor     bl,bl
                cmp     [eax],bl
                jle     L000107C9
L0001077C:
                call    jmp_ntoskrnl.exe!KeGetCurrentThread
                push    00000001h
                mov     cl,bl
                pop     edx
```

```
                shl     edx,cl
                push    edx
                push    eax
                call    jmp_ntoskrnl.exe!KeSetAffinityThread
                mov     eax,[L00010F68]
                mov     eax,[eax+02h]
                cli
                mov     edx,[L00010F60]
                mov     cx,[L00011198]
                mov     [eax+edx*8],cx
                mov     ecx,[L00011198]
                mov     edx,[L00010F60]
                shr     ecx,10h
                mov     [eax+edx*8+06h],cx
                sti
                mov     eax,[ntoskrnl.exe!KeNumberProcessors]
                inc     bl
                cmp     bl,[eax]
                jl      L0001077C
L000107C9:
                call    jmp_ntoskrnl.exe!KeGetCurrentThread
                mov     ecx,[ntoskrnl.exe!KeNumberProcessors]
                push    00000001h
                pop     edx
                mov     cl,[ecx]
                shl     edx,cl
                dec     edx
                push    edx
                push    eax
                call    jmp_ntoskrnl.exe!KeSetAffinityThread
                and     dword ptr [L00011124],00000000h
                xor     eax,eax
                pop     ebx
                retn
;------------------------------------------------------------------------------
SUB_L000107EE:
                sidt    [L000111F0]
                mov     eax,[L00010F68]
                mov     ecx,[L00010F60]
                mov     eax,[eax+02h]
                lea     ecx,[eax+ecx*8]
                movzx   eax,[ecx+06h]
                movzx   ecx,[ecx]
                shl     eax,10h
                or      eax,ecx
                cmp     eax,L000102C0
                mov     [L00011184],eax
                jnz     L00010822
                push    00000001h
```

```
                pop     eax
                retn
;-------------------------------------------------------------------------------
 L00010822:
                mov     [L00011138],eax
                xor     eax,eax
                retn
;-------------------------------------------------------------------------------
 L0001082A:
                call    SUB_L000107EE
                test    eax,eax
                jnz     L00010853
                mov     dword ptr [L0001113C],00000001h
                call    SUB_L000106E2
                push    00000000h
                push    00000000h
                push    L00011160
                call    [ntoskrnl.exe!KeInsertQueueDpc]
                jmp     L0001085A
 L00010853:
                and     dword ptr [L0001113C],00000000h
 L0001085A:
                retn    0008h
;-------------------------------------------------------------------------------
                Align   2
 SUB_L0001085E:
                push    ebp
                mov     ebp,esp
                call    SUB_L00010D14
                sidt    [L000111F0]
                mov     eax,[L00010F68]
                mov     ecx,[L00010F60]
                push    [ebp+08h]
                mov     eax,[eax+02h]
                push    L0001062C
                push    L00011160
                lea     eax,[eax+ecx*8]
                movzx   ecx,[eax+06h]
                movzx   eax,[eax]
                shl     ecx,10h
                or      ecx,eax
                mov     [L00011198],ecx
                call    [ntoskrnl.exe!KeInitializeDpc]
                push    00000000h
                push    L0001082A
                push    [ebp+08h]
                call    [ntoskrnl.exe!IoInitializeTimer]
                neg     eax
                sbb     eax,eax
```

```
                and     eax,C0000001h
                pop     ebp
                retn    0004h
;-------------------------------------------------------------------------
 SWC000108C0__Device_Psmkb2k:
                unicode         '\Device\Psmkb2k',0000h
 SWC000108E0__DosDevices_Psmkb2k:
                unicode         '\DosDevices\Psmkb2k',0000h

;-------------------------------------------------------------------------------------------------------------------------
Driver entry point:
 EntryPoint:
                push    ebp
                mov     ebp,esp
                sub     esp,0000005Ch
                push    esi
                push    edi
                push    00000008h
                mov     esi,SWC000108C0__Device_Psmkb2k //Device\Driver constant
                pop     ecx
                lea     edi,[ebp-34h]
                and     dword ptr [ebp-04h],00000000h
                push    0000000Ah
                rep movsd
                pop     ecx
                lea     eax,[ebp-34h]
                mov     esi,SWC000108E0__DosDevices_Psmkb2k //DosDevice\Driver constant
                lea     edi,[ebp-5Ch]
                push    eax
                lea     eax,[ebp-0Ch]
                rep movsd
                mov     esi,[ntoskrnl.exe!RtlInitUnicodeString]  // Convert to Unicode name
                push    eax
                call    esi
                mov     edi,[ebp+08h]
                lea     eax,[ebp-04h]
                push    eax
                push    00000000h
                push    00000000h
                lea     eax,[ebp-0Ch]
                push    00008300h
                push    eax
                push    00000000h
                push    edi
                call    [ntoskrnl.exe!IoCreateDevice]          //Call IoCreate Device to Create DevObj
                test    eax,eax
                jl      L000109C1
                lea     eax,[ebp-5Ch]
                push    eax
```

```
                lea     eax,[ebp-14h]
                push    eax
                call    esi
                lea     eax,[ebp-0Ch]
                push    eax
                lea     eax,[ebp-14h]
                push    eax
                call    [ntoskrnl.exe!IoCreateSymbolicLink]    // Create symbolic name for DevObj
                push    [ebp-04h]
                mov     esi,eax
                test    esi,esi
                jge     L0001098A                              //??? go to  L0001098A for DelDevObj
                call    [ntoskrnl.exe!IoDeleteDevice]
L00010986:                                      // Label for going
                mov     eax,esi
                jmp     L000109C1
L0001098A:                                      // Procedure for Deleting DevObj
                call    SUB_L0001085E
                mov     esi,eax
                test    esi,esi
                jge     L000109AA
                push    [ebp-04h]
                call    [ntoskrnl.exe!IoDeleteDevice]
                lea     eax,[ebp-14h]
                push    eax
                call    [ntoskrnl.exe!IoDeleteSymbolicLink]
                jmp     L00010986
L000109AA:
                mov     eax,L000109C8
                mov     dword ptr [edi+34h],L00010CC6
                mov     [edi+70h],eax
                mov     [edi+40h],eax
                mov     [edi+38h],eax
                xor     eax,eax
L000109C1:
                pop     edi
                pop     esi
                leave
                retn    0008h
;-------------------------------------------------------------------------------EVENT WORKING----------
                Align   4
L000109C8:                      //Proc  -  Event  working
                push    ebp
                mov     ebp,esp
                push    ebx
                mov     ebx,[ebp+0Ch]
                push    esi
                push    edi
                mov     eax,[ebx+60h]
```

```
                mov     esi,[ebx+0Ch]
                xor     edi,edi
                mov     [ebx+18h],edi
                mov     [ebx+1Ch],edi
                cmp     byte ptr [eax],0Eh
                mov     edx,[eax+08h]
                jnz     L00010C87
                mov     eax,[eax+0Ch]
                mov     ecx,830020E0h
                cmp     eax,ecx
                ja      L00010BCB
                jz      L00010BBF
                cmp     eax,830020C4h
                jz      L00010B9C
                cmp     eax,830020C8h
                jz      L00010B0D
                cmp     eax,830020CCh
                jz      L00010A71
                cmp     eax,830020D8h
                jz      L00010A44
                cmp     eax,830020DCh
                jnz     L00010BF6
                push    edi
                push    00000002h
                push    [L00011188]
                call    [ntoskrnl.exe!KeSetEvent]
                jmp     L00010C87
L00010A44:
                cmp     edx,00000004h
                jc      L00010C87
                push    edi
                push    L00011188
                push    00000001h
                push    edi
                push    00000002h
                push    [esi]
                call    [ntoskrnl.exe!ObReferenceObjectByHandle]
                push    [L00011188]
                call    [ntoskrnl.exe!KeClearEvent]
                jmp     L00010C87
L00010A71:
                call    SUB_L00010DEC
                cmp     eax,FFFFFFFFh
                mov     [L00011144],eax
                jz      L00010A93
                cmp     [L00011108],edi
                jnz     L00010A93
                push    eax
                call    SUB_L00010604
```

```
                mov     [L00011144],eax
L00010A93:
                cmp     dword ptr [L0001113C],00000001h
                jnz     L00010AA6
                mov     dword ptr [L00011144],00000100h
L00010AA6:
                xor     eax,eax
                mov     edi,esi
                stosd
                mov     eax,[L00011144]
                mov     [esi],eax
                mov     eax,[ntoskrnl.exe!KeTickCount]
                mov     [ebp+08h],eax
L00010ABA:
                mov     eax,[ebp+08h]
                mov     eax,[eax+04h]
                mov     [L00011194],eax
                mov     ecx,[ebp+08h]
                mov     ecx,[ecx]
                mov     [L00011190],ecx
                mov     ecx,[ebp+08h]
                cmp     eax,[ecx+08h]
                jz      L00010ADC
                pause                           ; SSE2
                jmp     L00010ABA
L00010ADC:
                xor     eax,eax
                mov     dword ptr [ebx+1Ch],00000004h
                cmp     [L00011114],eax
                jle     L00010C87
                push    eax
                push    eax
                push    L00011160
                mov     dword ptr [L00011180],FFFFFFFEh
                call    [ntoskrnl.exe!KeInsertQueueDpc]
                jmp     L00010C87
L00010B0D:
                push    00000001h
                mov     [L00011120],edi
                pop     eax
                xor     ecx,ecx
                cmp     [esi],eax
                mov     [L0001111C],eax
                mov     eax,[ntoskrnl.exe!KeTickCount]
                setz    cl
                mov     [L00011128],ecx
                mov     [ebp+08h],eax
L00010B30:
                mov     eax,[ebp+08h]
```

```
                mov     eax,[eax+04h]
                mov     [L000111EC],eax
                mov     ecx,[ebp+08h]
                mov     ecx,[ecx]
                mov     [L000111E8],ecx
                mov     ecx,[ebp+08h]
                cmp     eax,[ecx+08h]
                jz      L00010B52
                pause                           ; SSE2
                jmp     L00010B30
L00010B52:
                mov     eax,[ntoskrnl.exe!KeTickCount]          // Number of times of Interrupts
                mov     [ebp+08h],eax
L00010B5A:
                mov     eax,[ebp+08h]
                mov     eax,[eax+04h]
                mov     [L00011194],eax
                mov     ecx,[ebp+08h]
                mov     ecx,[ecx]
                mov     [L00011190],ecx
                mov     ecx,[ebp+08h]
                cmp     eax,[ecx+08h]
                jz      L00010B7C
                pause                           ; SSE2
                jmp     L00010B5A
L00010B7C:
                push    00000010h
                xor     eax,eax
                pop     ecx
                mov     edi,L000111A0
                rep stosd
                mov     [L00011114],eax
                mov     [L00011110],eax
                mov     [L0001110C],eax
                jmp     L00010C87
L00010B9C:
                mov     ecx,[L00011188]
                mov     [L0001111C],edi
                call    [ntoskrnl.exe!ObfDereferenceObject]
                mov     [L0001113C],edi
                mov     [L00011180],edi
                jmp     L00010C87
L00010BBF:
                xor     eax,eax
                mov     edi,esi
                stosd
                mov     eax,[L00011124]
                jmp     L00010C0C
L00010BCB:
```

```
                cmp     eax,830020E4h
                jz      L00010C70
                cmp     eax,830020E8h
                jz      L00010C61
                cmp     eax,830020ECh
                jz      L00010C2F
                cmp     eax,830020F0h
                jz      L00010C17
                cmp     eax,830020F4h
                jz      L00010C02
L00010BF6:
                mov     dword ptr [ebx+18h],C000000Dh
                jmp     L00010C87
L00010C02:
                xor     eax,eax
                mov     edi,esi
                stosd
                mov     eax,[L00011138]
L00010C0C:
                mov     [esi],eax
                mov     dword ptr [ebx+1Ch],00000004h
                jmp     L00010C87
L00010C17:
                cmp     [L00011124],edi
                jz      L00010C87
                call    SUB_L00010770
                push    [ebp+08h]
                call    [ntoskrnl.exe!IoStopTimer]              // with Timer
                jmp     L00010C87
L00010C2F:
                cmp     edx,00000198h
                mov     [L00011108],edi
                jc      L00010C49
                push    00000066h
                mov     edi,L00010F70
                pop     ecx
                rep movsd
                xor     edi,edi
L00010C49:
                cmp     [L00011124],edi
                jnz     L00010C87
                call    SUB_L000106E2
                push    [ebp+08h]
                call    [ntoskrnl.exe!IoStartTimer]
                jmp     L00010C87
L00010C61:
                cmp     [L00011124],edi
                jz      L00010C87
                call    SUB_L00010770
```

```
                jmp     L00010C87
L00010C70:
                cmp     [L00011124],edi
                mov     dword ptr [L00011108],00000001h
                jnz     L00010C87
                call    SUB_L000106E2
L00010C87:
                mov     esi,[ebx+18h]
                xor     dl,dl
                mov     ecx,ebx
                call    [ntoskrnl.exe!IofCompleteRequest]
                mov     eax,esi
                pop     edi
                pop     esi
                pop     ebx
                pop     ebp
                retn    0008h
;------------------------------------------------------------------END OF EVENT WORKING----------------
;-------------------------------------------------------------**Procedure Implementations** ----------------------------
                Align   2
L00010C9E:                              // String constant: \DosDevices\Psmkb2k
db      5Ch;  '\'                       db      69h;  'i'       db      6Dh;  'm'
                db      00h;            db      00h;            db      00h;
                db      44h;  'D'       db      63h;  'c'       db      6Bh;  'k'
                db      00h;            db      00h;            db      00h;
                db      6Fh;  'o'       db      65h;  'e'       db      62h;  'b'
                db      00h;            db      00h;            db      00h;
                db      73h;  's'       db      73h;  's'       db      32h;  '2'
                db      00h;            db      00h;            db      00h;
                db      44h;  'D'       db      5Ch;  '\'       db      6Bh;  'k'
                db      00h;            db      00h;            db      00h;
                db      65h;  'e'       db      50h;  'P'       db      00h;
                db      00h;            db      00h;            db      00h;
                db      76h;  'v'       db      73h;  's'
                db      00h;            db      00h;
L00010CC6:
                push    ebp
                mov     ebp,esp
                sub     esp,00000030h
                push    esi
                cmp     dword ptr [L00011124],00000000h
                push    edi
                push    0000000Ah
                pop     ecx
                mov     esi,L00010C9E
                lea     edi,[ebp-30h]
                rep movsd
                pop     edi
                pop     esi
```

```
                jz      L00010CEB
                call    SUB_L00010770
L00010CEB:
                lea     eax,[ebp-30h]
                push    eax
                lea     eax,[ebp-08h]
                push    eax
                call    [ntoskrnl.exe!RtlInitUnicodeString]
                lea     eax,[ebp-08h]
                push    eax
                call    [ntoskrnl.exe!IoDeleteSymbolicLink]
                mov     eax,[ebp+08h]
                push    [eax+04h]
                call    [ntoskrnl.exe!IoDeleteDevice]
                leave
                retn    0004h
;-----------------------------------------------------------------------------
                Align   4
SUB_L00010D14:
                push    ebp
                mov     ebp,esp
                sub     esp,00000010h
                push    ebx
                push    esi
                xor     esi,esi
                push    edi
                mov     edi,[ntoskrnl.exe!IoQueryDeviceDescription]
                mov     [ebp-08h],esi
                mov     ebx,L00010D8A
L00010D2D:
                mov     eax,[ebp-08h]
                mov     dword ptr [ebp-10h],00000016h
                mov     [ebp-0Ch],eax
                mov     [ebp-04h],esi
L00010D3D:
                push    esi
                push    ebx
                push    esi
                push    esi
                push    esi
                lea     eax,[ebp-04h]
                push    esi
                push    eax
                lea     eax,[ebp-0Ch]
                push    eax
                call    edi
                cmp     eax,esi
                jl      L00010D74
                push    esi
```

```
                push    ebx
                push    esi
                push    esi
                lea     eax,[ebp-10h]
                push    esi
                push    eax
                lea     eax,[ebp-04h]
                push    eax
                lea     eax,[ebp-0Ch]
                push    eax
                call    edi
                cmp     eax,esi
                jge     L00010D6F
                cmp     eax,C0000034h
                jnz     L00010D84
L00010D6F:
                inc     [ebp-04h]
                jmp     L00010D3D
L00010D74:
                cmp     eax,C0000034h
                jnz     L00010D84
                inc     [ebp-08h]
                cmp     dword ptr [ebp-08h],00000010h
                jl      L00010D2D
L00010D84:
                pop     edi
                pop     esi
                pop     ebx
                leave
                retn
;--------------------------------------------------------------------------
                Align   2
L00010D8A:
                push    ebp
                mov     ebp,esp
                push    ecx
                mov     eax,[ebp+24h]
                push    ebx
                xor     ebx,ebx
                push    esi
                cmp     eax,ebx
                jz      L00010DE4
                mov     eax,[eax+04h]
                mov     esi,[eax+08h]
                add     esi,eax
                cmp     [esi+0Ch],ebx
                jbe     L00010DE4
                push    edi
                lea     edi,[esi+14h]
```

```
L00010DAA:
                movzx eax,[edi-04h]
                dec     eax
                dec     eax
                jnz     L00010DDA
                lea     eax,[ebp-04h]
                push    eax
                lea     eax,[ebp+27h]
                push    eax
                push    [edi+04h]
                push    [edi]
                push    [ebp+14h]
                push    [ebp+10h]
                call    [HAL.dll!HalGetInterruptVector]
                mov     [L00010F64],eax
                and     eax,000000FFh
                mov     [L00010F60],eax
L00010DDA:
                inc     ebx
                add     edi,00000010h
                cmp     ebx,[esi+0Ch]
                jc      L00010DAA
                pop     edi
L00010DE4:
                pop     esi
                xor     eax,eax
                pop     ebx
                leave
                retn    002Ch
;-----------------------------------------------------------------------------
SUB_L00010DEC:
                mov     ecx,[L00011110]
                cmp     ecx,[L0001110C]
                jnz     L00010DFD
                xor     eax,eax
                retn
;-----------------------------------------------------------------------------
L00010DFD:
                mov     eax,[L000111A0+ecx*4]
                inc     ecx
                cmp     ecx,00000010h
                mov     [L00011110],ecx
                jnz     L00010E17
                and     dword ptr [L00011110],00000000h
L00010E17:
                dec     [L00011114]
                retn
;-----------------------------------------------------------------------------
SUB_L00010E1E:
```

```
                mov     eax,[L0001110C]
                mov     ecx,[esp+04h]
                mov     [L000111A0+eax*4],ecx
                inc     eax
                cmp     eax,00000010h
                mov     [L0001110C],eax
                jnz     L00010E40
                and     dword ptr [L0001110C],00000000h
L00010E40:
                inc     [L00011114]
                retn    0004h
;-------------------------------------------------------------------------
                Align   2
jmp_ntoskrnl.exe!_allmul:
                jmp     [ntoskrnl.exe!_allmul]
jmp_ntoskrnl.exe!KeSetAffinityThread:
                jmp     [ntoskrnl.exe!KeSetAffinityThread]
jmp_ntoskrnl.exe!KeGetCurrentThread:
                jmp     [ntoskrnl.exe!KeGetCurrentThread]
jmp_HAL.dll!HalBeginSystemInterrupt:
                jmp     [HAL.dll!HalBeginSystemInterrupt]
jmp_HAL.dll!HalEndSystemInterrupt:
                jmp     [HAL.dll!HalEndSystemInterrupt]
;-------------------------------------------------------------------------
                00000018h DUP (??)
;-------------------------------------------------------------------------
;  Name: .rdata (Data Section)
;  Virtual Address:    00010E80h  Virtual Size:    000000C4h
;  Pointer To RawData: 00000E80h  Size Of RawData: 000000E0h
;
HAL.dll!HalEndSystemInterrupt:
                dd      ??
HAL.dll!HalBeginSystemInterrupt:
                dd      ??
HAL.dll!HalGetInterruptVector:
                dd      ??
                dd      00000000
ntoskrnl.exe!_allmul:
                dd      ??
ntoskrnl.exe!KeSetAffinityThread:
                dd      ??
ntoskrnl.exe!KeGetCurrentThread:
                dd      ??
ntoskrnl.exe!KeNumberProcessors:
                dd      ??
ntoskrnl.exe!IoInitializeTimer:
                dd      ??
ntoskrnl.exe!KeInitializeDpc:
                dd      ??
ntoskrnl.exe!IoDeleteSymbolicLink:
                dd      ??
ntoskrnl.exe!IoDeleteDevice:
                dd      ??
ntoskrnl.exe!IoCreateSymbolicLink:
                dd      ??
ntoskrnl.exe!KeQueryTimeIncrement:
                dd      ??
ntoskrnl.exe!RtlInitUnicodeString:
                dd      ??
ntoskrnl.exe!IofCompleteRequest:
                dd      ??
ntoskrnl.exe!IoStartTimer:
                dd      ??
ntoskrnl.exe!IoStopTimer:
                dd      ??
ntoskrnl.exe!ObfDereferenceObject:
                dd      ??
ntoskrnl.exe!KeClearEvent:
```

```
                dd      ??
ntoskrnl.exe!ObReferenceObjectByHandle:
                dd      ??
ntoskrnl.exe!IoQueryDeviceDescription:
                dd      ??
ntoskrnl.exe!KeTickCount:
                dd      ??
ntoskrnl.exe!KeSetEvent:
                dd      ??
ntoskrnl.exe!IoCreateDevice:
                dd      ??
ntoskrnl.exe!KeInsertQueueDpc:
                dd      ??
                dd      00000000
                db      00h;
                db      00h;
                db      00h;
                db      00h;
                dd      00000000h
                dd      40729955h
                dw      0000h
                dw      0000h
                dd      00000004h
                dd      00000110h
                dd      00000000h
                dd      00001B00h
                dd      00000000h
                dd      40729955h
                dw      0000h
                dw      0000h
                dd      00000003h
                dd      000000F0h
                dd      00000000h
                dd      00001C10h
                dd      00000000h
                dd      40729955h
                dw      0000h
                dw      0000h
                dd      00000002h
                dd      0000003Fh
                dd      00000000h
                dd      00001D00h

`;-----------------------------------------------------------------------
                0000001Ch DUP (??);
;-----------------------------------------------------------------------
;  Name: .data
;  Virtual Address:    00010F60h  Virtual Size:    00000296h
;  Pointer To RawData: 00000F60h  Size Of RawData: 000002A0h
;
L00010F60:
                dd      00000031h
L00010F64:
                db      31h;   '1'
                db      00h;
                db      00h;
                db      00h;
L00010F68:
                dd      L000111F0
                db      00h;
                db      00h;
                db      00h;
                db      00h;
L00010F70:
                db      29h;   ')'
                db      00h;
                db      00h;
                db      00h;
L00010F74:
                dd      00000001h
                db      02h;
                db      00h;
                db      00h;
                db      00h;
                db      08h;
                db      00h;
                db      00h;
                db      00h;
                db      03h;
                db      00h;
                db      00h;
                db      00h;
                db      09h;
                db      00h;
                db      00h;
                db      00h;
                db      04h;
                db      00h;
                db      10h;
                db      00h;
                db      00h;
                db      00h;
                db      00h;
                db      05h;
                db      00h;
                db      00h;
                db      00h;
                db      11h;
                db      00h;
                db      00h;
                db      00h;
                db      06h;
                db      00h;
                db      00h;
                db      00h;
                db      00h;
```

```
db      18h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      14h;
db      00h;                    db      0Dh;                    db      00h;
db      07h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      12h;
db      00h;                    db      2Dh;    '-'             db      00h;
db      19h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      15h;
db      00h;                    db      2Bh;    '+'             db      00h;
db      08h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      17h;
db      00h;                    db      2Eh;    '.'             db      00h;
db      21h;    '!'             db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      16h;
db      00h;                    db      10h;                    db      00h;
db      09h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      1Ah;
db      00h;                    db      02h;                    db      00h;
db      1Dh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      17h;
db      00h;                    db      11h;                    db      00h;
db      0Ah;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      22h;    '"'
db      00h;                    db      07h;                    db      00h;
db      25h;    '%'             db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      18h;
db      00h;                    db      12h;                    db      00h;
db      0Bh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      1Eh;
db      00h;                    db      0Ah;                    db      00h;
db      28h;    '('             db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      19h;
db      00h;                    db      13h;                    db      00h;
db      0Ch;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      26h;    '&'
db      00h;                    db      0Fh;                    db      00h;
db      2Bh;    '+'             db      00h;                    db      00h;
```

```
db      00h;                    db      22h;  '"'               db      00h;
db      1Ah;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      2Ah;  '*'
db      00h;                    db      13h;                    db      00h;
db      29h;  ')'               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      2Ch;  ','
db      00h;                    db      23h;  '#'               db      00h;
db      1Bh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      16h;                    db      04h;
db      00h;                    db      00h;                    db      00h;
db      2Ch;  ','               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      24h;  '$'               db      2Dh;  '-'
db      00h;                    db      00h;                    db      00h;
db      1Eh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      05h;
db      00h;                    db      1Bh;                    db      00h;
db      03h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      2Eh;  '.'
db      00h;                    db      25h;  '%'               db      00h;
db      1Fh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      0Ch;
db      00h;                    db      23h;  '#'               db      00h;
db      06h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      2Fh;  '/'
db      00h;                    db      26h;  '&'               db      00h;
db      20h;  ' '               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      0Dh;
db      00h;                    db      1Fh;                    db      00h;
db      0Bh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      30h;  '0'
db      00h;                    db      27h;  '''               db      00h;
db      21h;  '!'               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      14h;
db      00h;                    db      27h;  '''               db      00h;
db      0Eh;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      31h;  '1'
db      00h;                    db      28h;  '('               db      00h;
```

```
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      30h;  '0'               db      00h;
db      15h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;        L00011130:
db      00h;                    db      4Eh;  'N'               dd      00000000h
db      32h;  '2'               db      00h;        L00011134:
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      33h;  '3'               db      00h;
db      1Ch;                    db      00h;                    db      00h;
db      00h;                    db      00h;        L00011138:
db      00h;                    db      00h;                    dd      00000000h
db      00h;                    db      39h;  '9'   L0001113C:
db      33h;  '3'               db      00h;                    dd      00000000h
db      00h;                    db      00h;        L00011140:
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      32h;  '2'   L00011141:
db      24h;  '$'               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;        L00011108:                      L00011144:
db      34h;  '4'               dd      00000000h               dd      00000000h
db      00h;        L0001110C:                                  db      00h;
db      00h;                    dd      00000000h               db      00h;
db      00h;        L00011110:                                  db      00h;
db      20h;  ' '               dd      00000000h               db      00h;
db      00h;        L00011114:                                  db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      35h;  '5'               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;        L00011118:                                  db      00h;
db      00h;                    dd      00000000h               db      00h;
db      2Fh;  '/'   L0001111C:                                  db      00h;
db      00h;                    dd      00000000h               db      00h;
db      00h;        L00011120:                                  db      00h;
db      00h;                    db      00h;                    db      00h;
db      37h;  '7'               db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;        L00011124:                                  db      00h;
db      31h;  '1'               dd      00000000h               db      00h;
db      00h;        L00011128:                                  db      00h;
db      00h;                    db      00h;                    db      00h;
db      00h;                    db      00h;                    db      00h;
db      4Ah;  'J'               db      00h;                    db      00h;
db      00h;                    db      00h;        L00011160://32 byte = DWORD
db      00h;        L0001112C:                                  db      00h;
```

```
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;    L00011198:                                      db      00h;
                db      00h;                    dd      00000000h               db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;    L000111A0:                                      db      00h;
                db      00h;                    dd      00000000h               db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;    L000111E0:
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;    L000111E4:
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
L00011180:                                      db      00h;                    db      00h;
                dd      00000000h               db      00h;                    db      00h;
L00011184:                                      db      00h;    L000111E8:
                db      00h;                    db      00h;                    dd      00000000h
                db      00h;                    db      00h;    L000111EC:
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
L00011188:                                      db      00h;                    db      00h;
                dd      00000000h               db      00h;                    db      00h;
                db      00h;                    db      00h;    L000111F0:
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
                db      00h;                    db      00h;                    db      00h;
L00011190:                                      db      00h;                    db      00h;
                dd      00000000h               db      00h;                    db      00h;
L00011194:                                      db      00h;                    db      00h;
                db      00h;                    db      00h;
```

```
;-------------------------------------------------------------------------
                0000000Ah DUP (??)
;
;-------------------------------------------------------------------------
;  Name: INIT
;  Virtual Address:    00011200h  Virtual Size:    000002C2h
;  Pointer To RawData: 00001200h  Size Of RawData: 000002E0h
;

dd      0000124Ch
        dd      00000000h
        dd      00000000h
        dd      00001462h
        dd      00000E90h
        dd      0000123Ch
        dd      00000000h
        dd      00000000h
        dd      000014BAh
        dd      00000E80h
        dd      00000000h
        dd      00000000h
        dd      00000000h
        dd      00000000h
        dd      00000000h
        dd      0000148Ah
        dd      00001470h
        dd      000014A2h
        dd      00000000h
        dd      000012F0h
        dd      000012FAh
        dd      00001310h
        dd      00001326h
        dd      0000133Ch
        dd      00001350h
        dd      00001362h
        dd      0000137Ah
        dd      0000138Ch
        dd      000012D8h
        dd      000013B6h
        dd      000013CEh
        dd      000013E4h
        dd      000013F4h
        dd      00001402h
        dd      0000141Ah
        dd      0000142Ah
        dd      00001446h
        dd      000012CAh
        dd      000012BCh
        dd      000013A4h
        dd      000012A8h
        dd      00000000h
        dw      01D0h
        db      'KeInsertQueueDpc',0
        db      00h
        dw      01F9h
        db      'KeSetEvent',0
        db      00h
        dw      020Bh
        db      'KeTickCount',0
        dw      01DDh
        db      'KeQueryTimeIncrement',0
        db      00h
        dw      046Ah
        db      '_allmul',0
        dw      01F6h
        db      'KeSetAffinityThread',0
        dw      01B2h
        db      'KeGetCurrentThread',0
        db      00h
        dw      01D4h
        db      'KeNumberProcessors',0
        db      00h
        dw      014Ch
        db      'IoInitializeTimer',0
        dw      01C1h
        db      'KeInitializeDpc',0
        dw      0127h
        db      'IoDeleteSymbolicLink',0
        db      00h
        dw      0125h
        db      'IoDeleteDevice',0
        db      00h
        dw      0121h
        db      'IoCreateSymbolicLink',0
        db      00h
```

```
                dw      011Bh                           db      'KeClearEvent',0
                db      'IoCreateDevice',0              db      00h
                db      00h                             dw      02B5h
                dw      0364h                           db
                db      'RtlInitUnicodeString',0    'ObReferenceObjectByHandle',0
                db      00h                             dw      0158h
                dw      0195h                           db
                db      'IofCompleteRequest',0      'IoQueryDeviceDescription',0
                db      00h                             db      00h
                dw      0181h                           db      'ntoskrnl.exe',0
                db      'IoStartTimer',0                db      00h
                db      00h                             dw      000Ah
                dw      0183h                           db      'HalBeginSystemInterrupt',0
                db      'IoStopTimer',0                 dw      0010h
                dw      02BAh                           db      'HalEndSystemInterrupt',0
                db      'ObfDereferenceObject',0        dw      0017h
                db      00h                             db      'HalGetInterruptVector',0
                dw      01A6h                           db      'HAL.dll',0
;-------------------------------------------------------------------------------
                0000001Eh DUP (??)
;-------------------------------------------------------------------------------
; Imports from ntoskrnl.exe
;
        extrn _allmul                           extrn KeClearEvent
        extrn KeSetAffinityThread               extrn ObReferenceObjectByHandle
        extrn KeGetCurrentThread                extrn IoQueryDeviceDescription
        extrn KeNumberProcessors                extrn KeTickCount
        extrn IoInitializeTimer                 extrn KeSetEvent
        extrn KeInitializeDpc                   extrn IoCreateDevice
        extrn IoDeleteSymbolicLink              extrn KeInsertQueueDpc
        extrn IoDeleteDevice                ;
        extrn IoCreateSymbolicLink          ; Imports from HAL.dll
        extrn KeQueryTimeIncrement          ;
        extrn RtlInitUnicodeString              extrn HalEndSystemInterrupt
        extrn IofCompleteRequest                extrn HalBeginSystemInterrupt
        extrn IoStartTimer                      extrn HalGetInterruptVector
        extrn IoStopTimer                   ;
        extrn ObfDereferenceObject
;-------------------------------------------------------------------------------
```