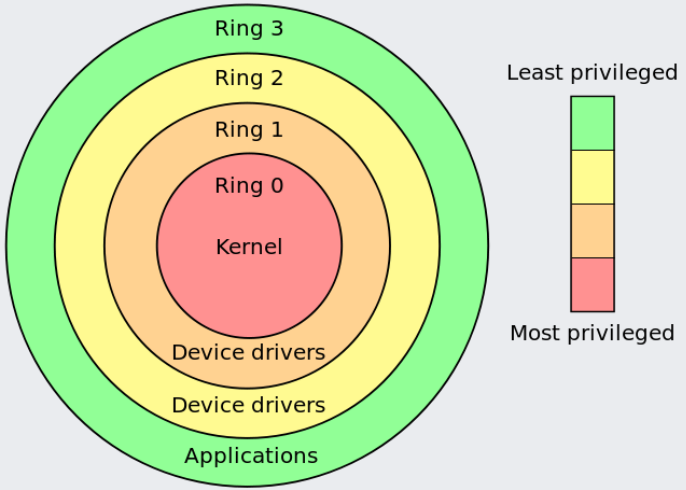
# Windows Kernel, Kernel Driver-y

*Robert Lipovský*

Základy Reverzného Inžinierstva 7.4.2016

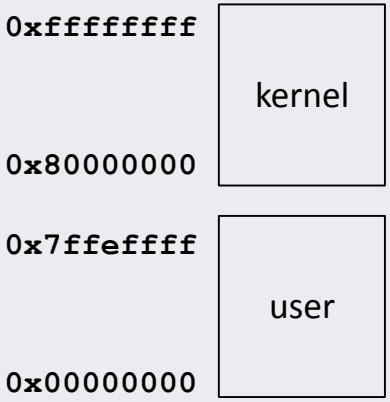
# Kernel? Kernel Mode? Ring 0?

- x86 podporuje 4 privilege levels – ring 0 – ring 3
- Windows používa 2:
  - user mode (ring 3) – kód aplikácií
  - kernel mode (ring 0) – system services, device drivers




- Kernel mode – prístup k celej pamäti a všetkým inštrukciám CPU

- Procesy majú vlastný adresný priestor
- Windows kernel a kód driverov zdieľaju jeden adresný priestor
  - na 32bit (bez PAE) 0x8000000 → 0xffffffff na x86



A problem has been detected and Windows has been shut down to prevent damage
to your computer.

IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

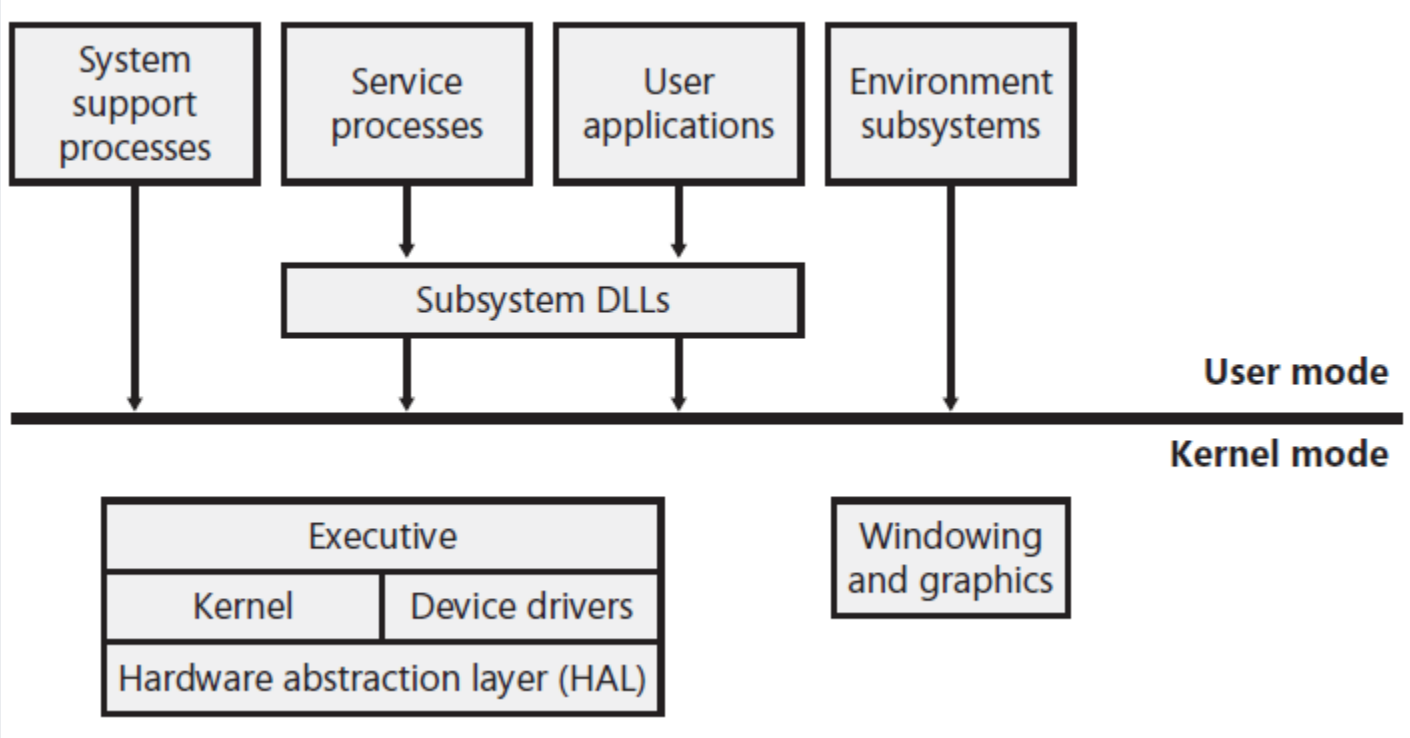
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical Information:

*** STOP: 0x00000001 (0x00000001, 0x00000001, 0x00000000, 0x00000000)

# Kernel? Kernel Mode? Ring 0?




** source: Windows Internals*

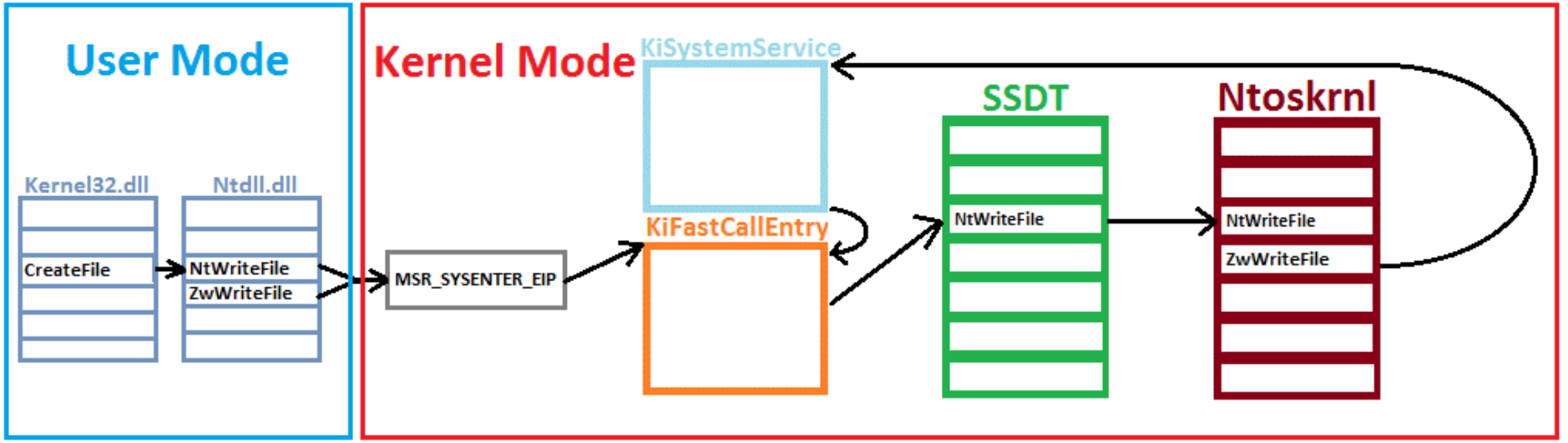
# Kernel, Executive, Drivery

- Windows kernel – jadro OS – časť *Ntoskrnl.exe* – nízkoúrovňové funkcie: thread scheduling, interrupt & exception dispatching, multiprocesorová synchronizácia

- Windows executive – horná časť *Ntoskrnl.exe* – základné služby OS –manažment pamäte, manažment threadov a procesov, power manažment, PnP, bezpečnosť, I/O, networking, kounikácia medzi procesmi a mnoho ďalších

- Drivery (ovládače) – hardware device drivery (prekladajú I/O volania do requestov pre konkrétne hw zariadenie) a nehardwarové device drivery (napr. filesystem, sieťové drivery, atď)
    - Frameworky: WDF (KMDF, UMDF). Starší WDM

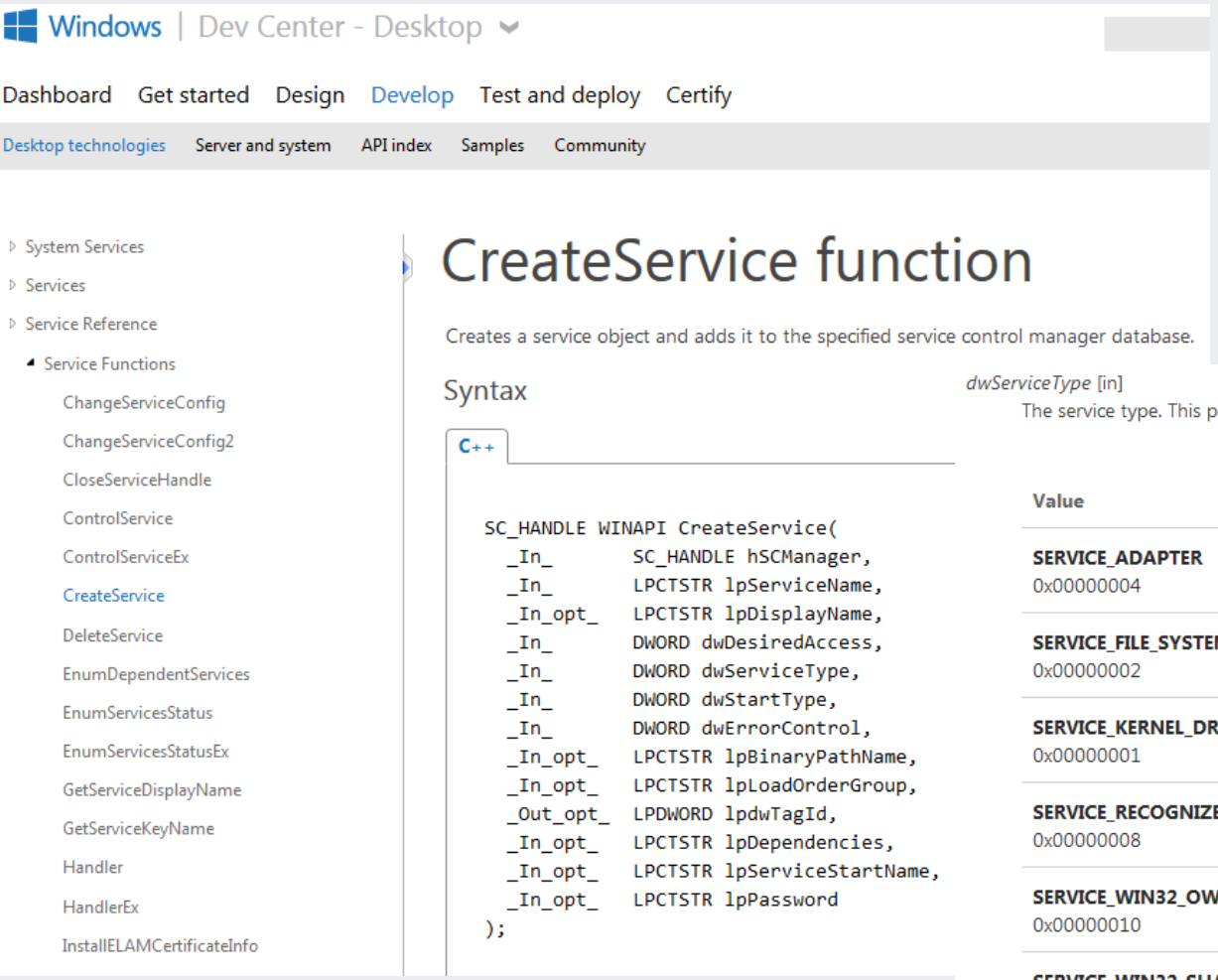
# Systémové volania (Native API)



# Driver Hello World ☺

- DEMO
- **Windows driver debugging with WinDbg and VMWare: https://briolidz.wordpress.com/2012/03/28/windows-driver-debugging-with-windbg-and-vmware/**
- **Driver Development Part 1: Introduction to Drivers http://www.codeproject.com/Articles/9504/Driver-Development-Part-Introduction-to-Drivers**

# Nie je service ako service...




*dwServiceType* [in]

The service type. This parameter can be one of the following values.

| Value | Meaning |
|---|---|
| **SERVICE_ADAPTER** 0x00000004 | Reserved. |
| **SERVICE_FILE_SYSTEM_DRIVER** 0x00000002 | File system driver service. |
| **SERVICE_KERNEL_DRIVER** 0x00000001 | Driver service. |
| **SERVICE_RECOGNIZER_DRIVER** 0x00000008 | Reserved. |
| **SERVICE_WIN32_OWN_PROCESS** 0x00000010 | Service that runs in its own process. |
| **SERVICE_WIN32_SHARE_PROCESS** 0x00000020 | Service that shares a process with one or more other services. For more information, see Service Programs. |

# Kernel Mode debugging

- Debugging Tools for Windows (súčasť WDK – Windows Driver Kit)
- Kd.exe, WinDbg
- Analýza crash dumpov
- Live remote debugging (2 počítače – target, host; cez kábel alebo pipe)
- Local kernel debugging

- Symboly!
- WinDbg CheatSheet: https://labs.snort.org/awbo/windbg.txt

Kernel 'com:pipe,port=\\.\pipe\stupidPipe,resets=0,reconnect' - WinDbg:6.11.0001.404 X86

File Edit View Debug Window Help

d:\projects\driver4preso\driver\driver.c

```
        RtlInitUnicodeString(&usSymbolicLink, symbolicLinkBuffer);
        IoDeleteSymbolicLink(&usSymbolicLink);
}

NTSTATUS OnCreate(IN PDEVICE_OBJECT theDeviceObject, IN PIRP Irp)
{
      //DbgPrint("OnCreate\n");
      return STATUS_SUCCESS;
}

NTSTATUS OnClose(IN PDEVICE_OBJECT theDeviceObject, IN PIRP Irp)
{
      //DbgPrint("OnClose\n");
      return STATUS_SUCCESS;
}

NTSTATUS OnDeviceIOControl(IN PDEVICE_OBJECT theDeviceObject, IN PIRP Irp)
{
     PIO_STACK_LOCATION irpStack;
     PVOID   inputBuffer;

     //DbgPrint("OnDeviceControl\n");

     irpStack = IoGetCurrentIrpStackLocation(Irp);
     inputBuffer = Irp->AssociatedIrp.SystemBuffer;

         DbgPrint("%s\n",inputBuffer);

         //Hide((int) *(int *)inputBuffer);

     Irp->IoStatus.Status = STATUS_SUCCESS;
     Irp->IoStatus.Information = 0;
     IoCompleteRequest(Irp, IO_NO_INCREMENT);

     return STATUS_SUCCESS;
}


NTSTATUS DriverEntry(IN PDRIVER_OBJECT theDriverObject, IN PUNICODE_STRING theRegistryPath)
{
```

Memory

Virtual: 0x820b5fb8 Display format: Byte Previous Next

```
820b5fb8 31 32 33 00 a0 35 5e 82 02 00 08 0a 4e 74 66 72 00 c3 53 82 d0 ec 0a 82 70 95  123..5^.....Ntfr..S.....p.
820b5fd2 5c 82 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  \.......................
820b5fec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 72 48 48 d3 07 00 00  ..........................SrHH....
820b6006 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........P...............
820b6020 00 00 00 00 20 e9 42 f8 dc ae 09 82 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....B...................
820b603a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6054 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b606e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6088 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b60a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b60bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b60d6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b60f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b610a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6124 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b613e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6158 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6172 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b618c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b61a6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b61c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b61da 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b61f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b620e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6228 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6242 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b625c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6276 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b6290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b62aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b62c4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b62de 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
820b62f8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
```

Disassembly

Offset: @$scopeip Previous Next

```
f8d37463 8bec            mov     ebp,esp
f8d37465 33c0            xor     eax,eax
f8d37467 5d              pop     ebp
f8d37468 c20800          ret     8
f8d3746b cc              int     3
f8d3746c cc              int     3
f8d3746d cc              int     3
f8d3746e cc              int     3
f8d3746f cc              int     3
driver4preso!OnDeviceIOControl:
f8d37470 8bff            mov     edi,edi
f8d37472 55              push    ebp
f8d37473 8bec            mov     ebp,esp
f8d37475 83ec08          sub     esp,8
f8d37478 8b450c          mov     eax,dword ptr [ebp+0Ch]
f8d3747b 50              push    eax
f8d3747c e84f000000      call    driver4preso!IoGetCurrentIrpStackLocation (f8d374d0)
f8d37481 8945f8          mov     dword ptr [ebp-8],eax
f8d37484 8b4d0c          mov     ecx,dword ptr [ebp+0Ch]
f8d37487 8b510c          mov     edx,dword ptr [ecx+0Ch]
f8d3748a 8955fc          mov     dword ptr [ebp-4],edx
f8d3748d 8b45fc          mov     eax,dword ptr [ebp-4] ss:0010:b197ac30=820b5fb8
f8d37490 50              push    eax
f8d37491 68e075d3f8      push    offset driver4preso! ?? ::FNODOBFM::`string' (f8d375e0)
f8d37496 e82f010000      call    driver4preso!DbgPrint (f8d375ca)
f8d3749b 83c408          add     esp,8
f8d3749e 8b4d0c          mov     ecx,dword ptr [ebp+0Ch]
f8d374a1 c7411800000000  mov     dword ptr [ecx+18h],0
f8d374a8 8b550c          mov     edx,dword ptr [ebp+0Ch]
f8d374ab c7421c00000000  mov     dword ptr [edx+1Ch],0
f8d374b2 32d2            xor     dl,dl
f8d374b4 8b4d0c          mov     ecx,dword ptr [ebp+0Ch]
f8d374b7 ff159076d3f8    call    dword ptr [driver4preso!_imp_IofCompleteRequest (f8d37690)]
f8d374bd 33c0            xor     eax,eax
f8d374bf 8be5            mov     esp,ebp
f8d374c1 5d              pop     ebp
f8d374c2 c20800          ret     8
f8d374c5 cc              int     3
f8d374c6 cc              int     3
f8d374c7 cc              int     3
f8d374c8 cc              int     3
f8d374c9 cc              int     3
```

Command

```
820b5ff8  00000000 00000000 48487253 0000007d
820b6008  00000000 00500000 00000000 00000000
820b6018  00000000 00000000 00000000 f842e920
820b6028  8209aedc 00000000 00000000 00000000
kd> db poi(inputBuffer)
820b5fb8  31 32 33 00 a0 35 5e 82-02 00 08 0a 4e 74 66 72  123..5^.....Ntfr
820b5fc8  00 c3 53 82 d0 ec 0a 82-70 95 5c 82 00 00 00 00  ..S.....p.\.....
820b5fd8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
820b5fe8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
820b5ff8  00 00 00 00 00 00 00 00-53 72 48 48 d3 07 00 00  ........SrHH....
820b6008  00 00 00 00 00 00 50 00-00 00 00 00 00 00 00 00  ......P.........
820b6018  00 00 00 00 00 00 00 00-00 00 00 00 20 e9 42 f8  ............ .B.
820b6028  dc ae 09 82 00 00 00 00-00 00 00 00 00 00 00 00  ................
kd> db *(inputBuffer)
Address expression missing from '*(inputBuffer)'
kd> db *((char*)inputBuffer)
Address expression missing from '*((char*)inputBuffer)'
kd> db poi(inputBuffer)
820b5fb8  31 32 33 00 a0 35 5e 82-02 00 08 0a 4e 74 66 72  123..5^.....Ntfr
820b5fc8  00 c3 53 82 d0 ec 0a 82-70 95 5c 82 00 00 00 00  ..S.....p.\.....
820b5fd8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
820b5fe8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
820b5ff8  00 00 00 00 00 00 00 00-53 72 48 48 d3 07 00 00  ........SrHH....
820b6008  00 00 00 00 00 00 50 00-00 00 00 00 00 00 00 00  ......P.........
820b6018  00 00 00 00 00 00 00 00-00 00 00 00 20 e9 42 f8  ............ .B.
820b6028  dc ae 09 82 00 00 00 00-00 00 00 00 00 00 00 00  ................
kd> g
123
OnUnload
```

*BUSY* Debuggee is running...

Registers

Customize...

| Reg | Value |
|---|---|
| gs | 0 |
| fs | 30 |
| es | 23 |
| ds | 23 |
| edi | 8242a6e0 |
| esi | 8240f2c0 |
| ebx | 8222b2e8 |
| edx | 820b5fb8 |
| ecx | 8222b2e8 |
| eax | 8222b358 |
| ebp | b197ac34 |
| eip | f8d3748d |
| cs | 8 |
| efl | 297 |
| esp | b197ac2c |
| ss | 10 |
| dr0 | 0 |
| dr1 | 0 |
| dr2 | 0 |
| dr3 | 0 |
| dr6 | ffff4ff0 |
| dr7 | 400 |
| di | a6e0 |
| si | f2c0 |
| bx | b2e8 |
| dx | 5fb8 |
| cx | b2e8 |
| ax | b358 |
| bp | ac34 |
| ip | 748d |
| fl | 297 |
| sp | ac2c |
| bl | e8 |
| dl | b8 |
| cl | e8 |
| al | 58 |
| bh | b2 |
| dh | 5f |
| ch | b2 |
| ah | b3 |
| fpcw | 0 |
| fpsw | 0 |
| fptw | 0 |
| fop... | 0 |
| fpip | b197a89c |
| fpi... | 0 |
| fpdp | b197a8f0 |
| fpd... | 0 |
| st0 | 0.000000000000 |
| st1 | -0.000000000000 |
| st2 | -0.000000000000 |
| st3 | 0.000000000000 |
| st4 | -0.000000000000 |
| st5 | 0.000000000000 |
| st6 | 0.000000000000 |
| st7 | -0.000000000000 |

Ln 40, Col 1 Sys 0:KdSrv:S Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM

# RET