SwishDbgExt

19th August 2014

SwishDbgExt is a Microsoft WinDbg debugging extension that expands the set of available commands by Microsoft WinDbg, but also fixes and improves existing commands.

This extension has been developed by Matt Suiche (@msuiche) – feel free to reach out on Twitter (even better, on the mailing list) to ask for more features, offer to contribute and/or report bugs.

Mailing-List: *https://groups.google.com/a/moonsols.com/forum/#!forum/dfir-list* or *dfir-list+subscribe@moonsols.com*

SwishDbgExt aims at making life easier for kernel developers, troubleshooters and security experts with a series of debugging, incident response and memory forensics commands.

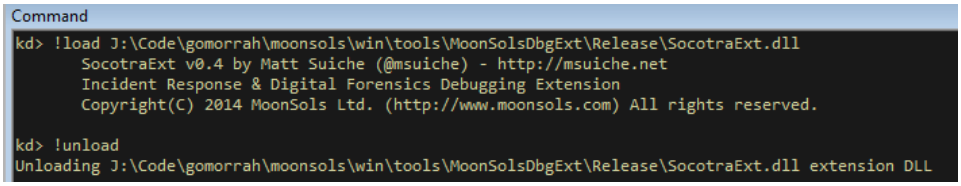
Because SwishDbgExt is a WinDbg debugging extension, it means it can be used on local or remote kernel debugging session, live sessions generated by Microsoft LiveKd, but also on Microsoft crash dumps generated to a Blue Screen of Death or hybrid utilities such as MoonSols DumpIt.

This is documentation is short and will be improved over time.

Installation

You can either copy the WinDbg extension in the corresponding (x86 or x64) WinDbg folder or load it manually using the !load command such as below. Please note you can't have spaces or quotes in the full path to the target dll to be loaded.

!load X:\FullPath\SwishDbgExt.dll



If you wish to update your WinDbg template with a more DML-friendly template, you can directly import windbg_template.reg file joined to the package.

Acknowledgements

Thanks to Frank Boldewin for his feedback and sharing his shellcode scanning techniques (!ms_malscore).

Thanks to Benjamin Delpy for his feedback and writing mimikatz (!ms_credentials).

Thanks to Patrick Barker for helping on the help documentation.

Commands

!SwishDbgExt.help

This command will give you the list of all commands if you specify no argument, will give you the list of parameters for an existing command if specified as an argument.

```
Command
0: kd> !SwishDbgExt.help
Commands for J:\Code\gomorrah\moonsols\win\tools\MoonSolsDbgExt\x64\Release\SwishDbgExt.dll:
  !help           - Displays information on available extension commands
  !ms_callbacks   - Display callback functions
  !ms_consoles    - Display console command's history
  !ms_credentials - Display user's credentials (based on gentilwiki's mimikatz)

  !ms_drivers     - Display list of drivers
  !ms_dump        - Dump memory space on disk
  !ms_exqueue     - Display Ex queued workers
  !ms_gdt         - Display GDT
  !ms_hivelist    - Display list of registry hives
  !ms_idt         - Display IDT
  !ms_malscore    - Analyze a memory space and returns a Malware Score Index
                    (MSI) - (based on Frank Boldewin's work)
  !ms_mbr         - Scan Master Boot Record (MBR)
  !ms_netstat     - Display network information (sockets, connections, ...)
  !ms_object      - Display list of object
  !ms_process     - Display list of processes
  !ms_readkcb     - Read key control block
  !ms_readknode   - Read key node
  !ms_readkvalue  - Read key value
  !ms_services    - Display list of services
  !ms_ssdt        - Display service descriptor table (SDT) functions
  !ms_store       - Display information related to the Store Manager
                    (ReadyBoost)
  !ms_timers      - Display list of KTIMER
  !ms_vacbs       - Display list of cached VACBs
!help <cmd> will give more information for a particular command
```

!ms_process

!ms_process is an improved version of !process and !dml_proc

```
kd> !SocotraExt.help ms_process
!ms_process [/dlls] [/threads] [/vads] [/vars] [/exports] [/all] [/scan]
            [/pid <pid>] [/handles <handles>] [<expr>]
  <expr>
  /pid <pid> - Display process information for a given Process Id (space-delimited)
  /handles <handles> - Display handles belonging to process
                       type (optional) - Object type to filter (e.g. Mutant or
                       Key)
  /dlls - Display dlls belonging to process
  /threads - Display threads belonging to process
  /vads - Display VADs belonging to process
  /vars - Display environment variables
  /exports - Display exports belonging to process
  /all - Display or scan all
  /scan - Display only malicious artifacts
Display list of processes
```

One of the nice thing as you can notice below is the usage of DML (Debugger Markup Language) with the commands. All the underline commands are in fact links to commands.

```
Command
kd> !ms_process

Process:       System              (PID=0x   4) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    PDB:           ntkrnlpa.pdb
    Vendor:        Microsoft Corporation
    Version:       5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
    Description:   NT Kernel & System
    Sections:     .text, POOLMI, MISYSPTE, POOLCODE, .data, INITDATA, INITCONS, PAGE, PAGELK, PAGEVRFY, PAGEWMI, PAGEKD, PAGESPEC, PAGEHDLS, .edata, PAGEDATA, PAGECO

Process:       smss.exe            (PID=0x 224) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:          \Device\HarddiskVolume1\WINDOWS\system32\smss.exe
    PDB:           smss.pdb
    Commandline:   \SystemRoot\System32\smss.exe (0417ea48)
    Sections:     .text, .data, .rsrc, .reloc,

Process:       csrss.exe           (PID=0x 264) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:          \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe
    PDB:           csrss.pdb
    Commandline:   C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=
    Sections:     .text, .data, .rsrc, .reloc,

Process:       winlogon.exe        (PID=0x 284) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:          \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe
    Commandline:   winlogon.exe (062477b0)
    Sections:     .text, .data, .rsrc,

Process:       services.exe        (PID=0x 2b0) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:          \Device\HarddiskVolume1\WINDOWS\system32\services.exe
    PDB:           services.pdb
    Vendor:        Microsoft Corporation
    Version:       5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
    Description:   Services and Controller app
    Commandline:   C:\WINDOWS\system32\services.exe (04432908)
    Sections:     .text, .data, .rsrc,

Process:       lsass.exe           (PID=0x 2bc) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:          \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
    PDB:           lsass.pdb
    Commandline:   C:\WINDOWS\system32\lsass.exe (0419a8e8)
    Sections:     .text, .data, .rsrc,
```

As an example below, you can see the output of /vads /scan, to scan VAD (Virtual Address Descriptors). You can notice that one column gives the “Malware Score Index” which can be useful to detect shellcodes or heap-spray.

```
Command

Process:        AcroRd32.exe        (PID=0x 6d8) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:           \Device\HarddiskVolume1\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
    Commandline:    "C:\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe" /o (0418b768)
    Sections:       .text, .rdata, .data, .rsrc, .reloc,

    |----------------------|----------|-------------------|-------------------|-----------------------------------------------------------------------|
    | Protection           | MalScore | Start range       | End range         | FileObject                                                            |
    |----------------------|----------|-------------------|-------------------|-----------------------------------------------------------------------|
    |                      |        0 | 0x0000000000010000 | 0x0000000000011000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x0000000000020000 | 0x0000000000021000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_READWRITE |      702 | 0x0000000000030000 | 0x000000000004D000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x0000000000060000 | 0x000000000000E0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x00000000000E0000 | 0x0000000000120000 | (0xFFFFFFFF90909090)  |
    | MM_READONLY          |        0 | 0x0000000000130000 | 0x0000000000133000 | (0x0000000000000000)  |
    | MM_READONLY          |        0 | 0x0000000000140000 | 0x0000000000142000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x0000000000150000 | 0x0000000000153000 | (0x000000000004C0048) |
    | MM_READWRITE         |        0 | 0x0000000000160000 | 0x0000000000170000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x0000000000170000 | 0x0000000000180000 | (0x0000000000000000)  |
    | MM_READONLY          |        0 | 0x0000000000180000 | 0x0000000000196000 | (0xFFFFFFFF81F14590) \WINDOWS\system32\unicode.nls |
    | MM_READONLY          |        0 | 0x00000000001A0000 | 0x00000000001DD000 | (0xFFFFFFFF81E4F4B0) \WINDOWS\system32\locale.nls |
    | MM_READONLY          |        0 | 0x00000000001E0000 | 0x0000000000221000 | (0xFFFFFFFF81EBE028) \WINDOWS\system32\sortkey.nls |
    | MM_READONLY          |        0 | 0x0000000000230000 | 0x0000000000236000 | (0xFFFFFFFF822A4210) \WINDOWS\system32\sorttbls.nls |
    | MM_READWRITE         |        0 | 0x0000000000240000 | 0x0000000000340000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x0000000000340000 | 0x0000000000341000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x0000000000350000 | 0x0000000000351000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x0000000000360000 | 0x0000000000370000 | (0xFFFFFFFF90909090)  |
    | MM_READONLY          |        0 | 0x0000000000370000 | 0x0000000000373000 | (0xFFFFFFFF822DA598) \WINDOWS\system32\ctype.nls |
    | MM_READWRITE         |        0 | 0x0000000000380000 | 0x0000000000390000 | (0xFFFFFFFF90909090)  |
    | MM_READONLY          |        0 | 0x0000000000390000 | 0x0000000000392000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x00000000003A0000 | 0x00000000003B0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x00000000003B0000 | 0x00000000003C0000 | (0xFFFFFFFF90909090)  |
    | MM_READONLY          |        0 | 0x00000000003C0000 | 0x00000000003C2000 | (0x0000000000000000)  |
    | MM_READWRITE         |        0 | 0x00000000003D0000 | 0x00000000003E0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x00000000003E0000 | 0x00000000003F0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         |        0 | 0x00000000003F0000 | 0x0000000000400000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_WRITECOPY |     5884 | 0x0000000000400000 | 0x00000000000B6B000 | (0xFFFFFFFF82077868) \Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe |
    | MM_EXECUTE_READ      |        0 | 0x00000000000B70000 | 0x0000000000C38000 | (0x0000000000000000)  |
    | MM_READONLY          |        0 | 0x0000000000C40000 | 0x0000000000D43000 | (0x0000000000000000)  |
    | MM_EXECUTE_READ      |        0 | 0x0000000000D50000 | 0x0000000001050000 | (0x0000000000000000)  |
```

In the screenshot below, you can see an abnormally high score in several VADs – due to usage of heap spray. Just by clicking on the score it will run the scanning algorithm.

The scanning algorithm is based on Frank Boldewin's OfficeMalScanner utility.

```
    | MM_READWRITE         | 3638020 | 0x00000000061A0000 | 0x00000000065A0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x00000000065A0000 | 0x00000000069A0000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x00000000069A0000 | 0x0000000006DA0000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_WRITECOPY |     372 | 0x0000000007000000 | 0x0000000007028000 | (0xFFFFFFFF822160E8) \Program Files\Adobe\Acrobat 6.0\Reader\Bib.dll |
    | MM_READWRITE         | 3638020 | 0x0000000007030000 | 0x0000000007430000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x0000000007430000 | 0x0000000007830000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x0000000007830000 | 0x000000007C30000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_WRITECOPY |    2344 | 0x0000000008000000 | 0x00000000081B9000 | (0xFFFFFFFF81DEEAF8) \Program Files\Adobe\Acrobat 6.0\Reader\CoolType.dll |
    | MM_READWRITE         | 3638020 | 0x00000000081A0000 | 0x00000000085A0000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_WRITECOPY |     340 | 0x0000000008800000 | 0x0000000008882000 | (0xFFFFFFFF820ABC98) \Program Files\Adobe\Acrobat 6.0\Reader\JP2KLib.dll |
    | MM_READWRITE         | 3638020 | 0x0000000008890000 | 0x000000008C90000 | (0xFFFFFFFF90909090)  |
    | MM_EXECUTE_WRITECOPY |     332 | 0x0000000009000000 | 0x0000000009018000 | (0xFFFFFFFF81C79028) \Program Files\Adobe\Acrobat 6.0\Reader\OPP.dll |
    | MM_READWRITE         | 3638020 | 0x0000000009020000 | 0x0000000009420000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x0000000009420000 | 0x0000000009820000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x0000000009820000 | 0x000000009C20000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x000000009C20000 | 0x000000000A020000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x000000000A020000 | 0x000000000A420000 | (0x000000000004C0048) |
    | MM_READWRITE         | 3638020 | 0x000000000A420000 | 0x000000000A820000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x000000000A820000 | 0x000000000AC20000 | (0x000000000004C0048) |
    | MM_READWRITE         | 3638020 | 0x000000000AC20000 | 0x000000000B020000 | (0x000000000004C0048) |
    | MM_READWRITE         | 3638020 | 0x000000000B020000 | 0x000000000B420000 | (0x0000000000000000)  |
    | MM_READWRITE         | 3638020 | 0x000000000B420000 | 0x000000000B820000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x000000000B820000 | 0x000000000BC20000 | (0x000000000004C0048) |
    | MM_READWRITE         | 3638020 | 0x000000000BC20000 | 0x000000000C020000 | (0x000000000004C0048) |
    | MM_READWRITE         | 3638020 | 0x000000000C020000 | 0x000000000C420000 | (0xFFFFFFFF90909090)  |
    | MM_READWRITE         | 3638020 | 0x000000000C420000 | 0x000000000C820000 | (0x0000000000000688)  |
    | MM_READWRITE         | 3638020 | 0x000000000C820000 | 0x000000000CC20000 | (0xFFFFFFFF90909090)  |
```

And returns you information about where the shellcode is:

```
kd> !ms_malscore 0x000000000B420000 0x400000
   [ Base: 0x000000000B420000
   [ Size: 0x400000
    Heap-spray signature detected @ 0x20
    FS:[30h] signature @ 0x3FFEA8
    API-Hashing signature @ 0x3FFEF6
   -> Malware Score Index (MSI) = 3638020
kd> u 0xB81FEA8
0b81fea8 648b4030        mov     eax,dword ptr fs:[eax+30h]
0b81feac 780c            js      0b81feba
0b81feae 8b400c          mov     eax,dword ptr [eax+0Ch]
0b81feb1 8b701c          mov     esi,dword ptr [eax+1Ch]
0b81feb4 ad              lods    dword ptr [esi]
0b81feb5 8b5808          mov     ebx,dword ptr [eax+8]
0b81feb8 eb09            jmp     0b81fec3
0b81feba 8b4034          mov     eax,dword ptr [eax+34h]
```

/scan option can also be used on exported functions to know if the EAT (Export Address Table) has been patched or if the prolog of the function modified.

```
Command
kd> !ms_process /pid 0x6D8 /dlls /exports /scan

Process:       AcroRd32.exe        (PID=0x 6d8) | [+Dlls] [+Exports] [+Handles] [+Threads] [+VADs] [+Scan] [+Select context]
    Path:           \Device\HarddiskVolume1\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
    Commandline:    "C:\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe" /o (0423a1f0)
    Sections:      .text, .rdata, .data, .rsrc, .reloc,
    -> [  0]: (     ) C:\WINDOWS\system32\ntdll.dll
    |------|------|-------------------|-----------------------------------------------|---------|
    | Indx | Ord  | Addr              | Name                                          | Patched | Hooked |
    |------|------|-------------------|-----------------------------------------------|---------|
    | 1240 | 1240 | 0x000000007C901E1E | ceil                                          | No      | Hooked
ntdll!ceil:
7c901e1e e95af00600      jmp     ntdll!_ceil_default (7c970e7d)
7c901e23 8da42400000000  lea     esp,[esp]
7c901e2a 8d642400        lea     esp,[esp]
    | 1243 | 1243 | 0x000000007C901F5D | floor                                         | No      | Hooked
ntdll!floor:
7c901f5d e9f9f80600      jmp     ntdll!_floor_default (7c97185b)
7c901f62 8da42400000000  lea     esp,[esp]
7c901f69 8d642400        lea     esp,[esp]

    -> [  1]: (     ) C:\WINDOWS\system32\kernel32.dll
    |------|------|-------------------|-----------------------------------------------|---------|
    | Indx | Ord  | Addr              | Name                                          | Patched | Hooked |
    |------|------|-------------------|-----------------------------------------------|---------|
    |   50 |   50 | 0x000000007C8345E1 | CloseProfileUserMapping                       | No      | Hooked
kernel32!CloseProfileUserMapping:
7c8345e1 e83a7ffeff      call    kernel32!BaseDllFlushRegistryCache (7c81c520)
7c8345e6 833dd430887c00  cmp     dword ptr [kernel32!BaseDllIniUserKeyPath+0x4 (7c8830d4)],0
7c8345ed 7417            je      kernel32!CloseProfileUserMapping+0x25 (7c834606)
    |  118 |  118 | 0x000000007C859956 | DebugBreak                                    | No      | Hooked
kernel32!DebugBreak:
7c859956 e9705b0200      jmp     kernel32!DbgBreakPoint (7c87f4cb)
7c85995b 90              nop
7c85995c 90              nop
    |  470 |  470 | 0x000000007C81E685 | GetUserDefaultLangID                          | No      | Hooked
kernel32!GetUserDefaultLangID:
7c81e685 e936b9feff      jmp     kernel32!GetUserDefaultLCID (7c809fc0)
7c81e68a 804e0180        or      byte ptr [esi+1],80h
7c81e68e e98819ffff      jmp     kernel32!GlobalAlloc+0x170 (7c81001b)
    |  557 |  557 | 0x000000007C860940 | IsSystemResumeAutomatic                       | No      | Hooked
kernel32!IsSystemResumeAutomatic:
7c860940 ff15e813807c    call    dword ptr [kernel32!_imp__NtIsSystemResumeAutomatic (7c8013e8)]
7c860946 0fb6c0          movzx   eax,al
7c860949 c3              ret
```

Similar tests are available for the SSDT (!ms_ssdt).

!ms_ssdt

```
|   71 | 0xFFFFFFFFB240F3F2 | PROCMON20                                  |         |
|   72 | 0xFFFFFFFF8060CB34 | nt!NtEnumerateSystemEnvironmentValuesEx    |         |
|   73 | 0xFFFFFFFFB240F34E | PROCMON20                                  |         |
|   74 | 0xFFFFFFFF805A9126 | nt!NtExtendSection                         |         |
|   75 | 0xFFFFFFFF805E320E | nt!NtFilterToken                           |         |
|   76 | 0xFFFFFFFF8060C068 | nt!NtFindAtom                              |         |
|   77 | 0xFFFFFFFF8056BEE8 | nt!NtFlushBuffersFile                      |         |
|   78 | 0xFFFFFFFF805ABE38 | nt!NtFlushInstructionCache                 |         |
|   79 | 0xFFFFFFFFB240F446 | PROCMON20                                  |         |
|   80 | 0xFFFFFFFF805A1AB8 | nt!NtFlushVirtualMemory                    |         |
|   81 | 0xFFFFFFFF805ABDDA | nt!NtFlushWriteBuffer                      |  Yes    |
|   82 | 0xFFFFFFFF805AB94A | nt!NtFreeUserPhysicalPages                 |         |
|   83 | 0xFFFFFFFF805A8400 | nt!NtFreeVirtualMemory                     |         |
```

!ms_ssdt displays the System Service Dispatch Table. This command is extremely helpful in the investigation of suspected rootkit hooks through what is known as Direct Kernel Object Manipulation (DKOM). If you see a low level routine here that is hooked (such as nt!NtEnumerateKey), this can aid you in your analysis regarding a possible rootkit infection.

!ms_callbacks

```
kd> !ms_callbacks

[*] IopFsNotifyChangeQueueHead:
     Object: 0xFFFFFFFFE15036C8 Driver Object: 0xFFFFFFFF82096B20 Procedure: 0xFFFFFFFFF84BE876 (sr!SrFsNotification)
     Object: 0xFFFFFFFFE1ABC3C0 Driver Object: 0xFFFFFFFF81ED2F38 Procedure: 0xFFFFFFFFF84D54B8 (fltMgr!FltpFsNotification)
     Object: 0xFFFFFFFFE1BBA118 Driver Object: 0xFFFFFFFF820E54F8 Procedure: 0xFFFFFFFFB21D89EC (mrxnet)

[*] PnpProfileNotifyList/:
     Object: 0xFFFFFFFFE101B258 Driver Object: 0xFFFFFFFF823AFCE8 Session: 0x0 Procedure: 0xFFFFFFFF806027E4 (nt!WmipDockUndockEventCallback)
     Object: 0xFFFFFFFFE14B4EB8 Driver Object: 0xFFFFFFFF81E9DF38 Session: 0x0 Procedure: 0xFFFFFFFFF8761638 (i8042prt!I8xProfileNotificationCallback)

[*] PspCreateProcessNotifyRoutine:
     Procedure: 0xFFFFFFFFF87AD194 (vmci!VMCI_DeviceGet)
     Procedure: 0xFFFFFFFFB240CB94 (PROCMON20)

[*] PspLoadImageNotifyRoutine:
     Procedure: 0xFFFFFFFFB240CE4C (PROCMON20)
     Procedure: 0xFFFFFFFF805F81A6 (nt!WmipTraceLoadImage)
     Procedure: 0xFFFFFFFFF895AD06 (mrxcls)

[*] PspCreateThreadNotifyRoutine:
     Procedure: 0xFFFFFFFFB240CC9A (PROCMON20)

[*] CmpCallBackVector:

[*] KeBugCheckCallbackListHead:
     Procedure: 0xFFFFFFFFF83E65EF (NDIS!ndisBugcheckHandler)
     Procedure: 0xFFFFFFFF806D77CC (hal!HalpBugCheckCallback)
```

!ms_services

```
[200] | 0x01 |          | VMMEMCTL                        | Memory Control Driver                          | SERVICE_RUNNING  | \Driver\VMMEMCTL
[201] | 0x01 |          | vmmouse                         | VMware Pointing Device                         | SERVICE_RUNNING  | \Driver\vmmouse
[202] | 0x01 |          | vmscsi                          | vmscsi                                         | SERVICE_RUNNING  | \Driver\vmscsi
[204] | 0x10 | Pid=0x718 | VMUpgradeHelper                 | VMware Upgrade Helper                          | SERVICE_RUNNING  | "C:\Program Files\VMware\VMware Tools\VMUpgradeHelpe
[205] | 0x10 | Pid=0x34c | VMware Physical Disk Helper Service | VMware Physical Disk Helper Service            | SERVICE_RUNNING  | "C:\Program Files\VMware\VMware Tools\vmacthlp.ex
[206] | 0x01 |          | vmxnet                          | VMware Ethernet Adapter Driver                 | SERVICE_RUNNING  | \Driver\vmxnet
[207] | 0x01 |          | vmx_svga                        | vmx_svga                                       | SERVICE_RUNNING  | \Driver\vmx_svga
[208] | 0x01 |          | VolSnap                         | VolSnap                                        | SERVICE_RUNNING  | \Driver\VolSnap
[209] | 0x20 | Pid=0x408 | W32Time                         | Windows Time                                   | SERVICE_RUNNING  | C:\WINDOWS\System32\svchost.exe -k netsvcs
[210] | 0x01 |          | Wanarp                          | Remote Access IP ARP Driver                    | SERVICE_RUNNING  | \Driver\Wanarp
[211] | 0x01 |          | WDICA                           | WDICA                                          | SERVICE_STOPPED  |
[212] | 0x01 |          | wdmaud                          | Microsoft WINMM WDM Audio Compatibility Driver | SERVICE_RUNNING  | \Driver\wdmaud
[213] | 0x20 | Pid=0x4b0 | WebClient                       | WebClient                                      | SERVICE_RUNNING  | C:\WINDOWS\system32\svchost.exe -k LocalService
[214] | 0x20 | Pid=0x408 | winmgmt                         | Windows Management Instrumentation             | SERVICE_RUNNING  | C:\WINDOWS\System32\svchost.exe -k netsvcs
[215] | 0x01 |          | WS2IFSL                         | Windows Socket 2.0 Non-IFS Service Provider Support Environment | SERVICE_RUNNING  | \Driver\WS2IFSL
[216] | 0x20 | Pid=0x408 | wscsvc                          | Security Center                                | SERVICE_RUNNING  | C:\WINDOWS\System32\svchost.exe -k netsvcs
[217] | 0x20 | Pid=0x408 | wuauserv                        | Automatic Updates                              | SERVICE_RUNNING  | C:\WINDOWS\System32\svchost.exe -k netsvcs
[218] | 0x20 | Pid=0x408 | WZCSVC                          | Wireless Zero Configuration                    | SERVICE_RUNNING  | C:\WINDOWS\System32\svchost.exe -k netsvcs
```

!ms_readkcb
!ms_readknode

!reg WinDbg command has been a frustration for a long time, due to some bugs. This is why SwishDbgExt, has its own registry explorer functions to try to make access to registry data as simple as possible.

```
kd> !reg findkcb \REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES


Found KCB = e10345a8 :: \REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES

kd> !ms_readkcb e10345a8
 Key node Services¨ÿÿÿnk  contains 0 key values and 310 subkeys.

 [*] Subkeys (310):
   [ 0] 0xFFFFFFFFDA3524AC | .NET CLR Data
   [ 1] 0xFFFFFFFFDA355D0C | .NET CLR Networking
   [ 2] 0xFFFFFFFFDA351544 | .NET CLR Networking 4.0.0.0
   [ 3] 0xFFFFFFFFDA35AF44 | .NET Data Provider for Oracle
   [ 4] 0xFFFFFFFFDA356094 | .NET Data Provider for SqlServer
   [ 5] 0xFFFFFFFFDA35A67C | .NET Memory Cache 4.0
   [ 6] 0xFFFFFFFFDA3522FC | .NETFramework
   [ 7] 0xFFFFFFFFDA233C14 | Abiosdsk
   [ 8] 0xFFFFFFFFDA233D5C | abp480n5
   [ 9] 0xFFFFFFFFDA233F9C | ACPI
   [10] 0xFFFFFFFFDA234274 | ACPIEC
   [11] 0xFFFFFFFFDA23439C | adpu160m
```

```
  [309] 0xFFFFFFFFDA29EC24 | {9B5A1EAD-7852-455F-9740-5E1FCD05D812}
kd> !ms_readknode 0xFFFFFFFFE1035B60 0xFFFFFFFFDA37BB24
 Key node MRxNet contains 7 key values and 1 subkeys.

 [*] Values (7):
   [ 0] 0xFFFFFFFFDA37BB7C | Description                    |        MRXNET (REG_SZ)
   [ 1] 0xFFFFFFFFDA37BBBC | DisplayName                    |        MRXNET (REG_SZ)
   [ 2] 0xFFFFFFFFDA37BBFC | ErrorControl                   |        0x00000000 (REG_DWORD)
   [ 3] 0xFFFFFFFFDA37BC24 | Group                          |        Network (REG_SZ)
   [ 4] 0xFFFFFFFFDA37BC5C | ImagePath                      |        \??\C:\WINDOWS\system32\Drivers\mrxnet.sys (REG_SZ)
   [ 5] 0xFFFFFFFFDA37BCE4 | Start                          |        0x00000001 (REG_DWORD)
   [ 6] 0xFFFFFFFFDA37BD24 | Type                           |        0x00000001 (REG_DWORD)

 [*] Subkeys (1):
   [ 0] 0xFFFFFFFFE1193E1C | Enum
```

!ms_netstat

```
kd> !ms_netstat
    | Proto | Local Address            | Foreign address          | State       | Process Name     | Pid    | Creation time
    |-----------------------------------------------------------------------------------------------------------------------
    | UDP   |            0.0.0.0:62465 |                0.0.0.0:0 | LISTEN      |                  | 0x02a8 | 29/10/2010 17: 9: 5 (UTC)
    | TCP   |            0.0.0.0:48385 |                0.0.0.0:0 | LISTEN      |                  | 0x0004 | 29/10/2010 17: 8:53 (UTC)
    | TCP   |            0.0.0.0:34560 |                0.0.0.0:0 | LISTEN      |                  | 0x03ac | 29/10/2010 17: 8:55 (UTC)
    | TCP   |            127.0.0.1:260 |                0.0.0.0:0 | LISTEN      |                  | 0x00bc | 29/10/2010 17: 9: 9 (UTC)
    | UDP   |            0.0.0.0:29956 |                0.0.0.0:0 | LISTEN      |                  | 0x0438 | 31/10/2010 16:36:16 (UTC)
    | UKNWN |                0.0.0.0:0 |                0.0.0.0:0 | LISTEN      |                  | 0x02a8 | 29/10/2010 17: 9: 5 (UTC)
    | UDP   |            0.0.0.0:30212 |                0.0.0.0:0 | LISTEN      |                  | 0x0438 | 31/10/2010 16:36:16 (UTC)
    | UDP   |          127.0.0.1:27655 |                0.0.0.0:0 | LISTEN      |                  | 0x04b0 |  3/ 6/2011  4:25:47 (UTC)
    | UDP   |            0.0.0.0:37905 |                0.0.0.0:0 | LISTEN      |                  | 0x02a8 | 29/10/2010 17: 9: 5 (UTC)
    | TCP   |           127.0.0.1:8212 |                0.0.0.0:0 | LISTEN      |                  | 0x062c | 29/10/2010 17: 9: 5 (UTC)
```

!ms_store

The present command allows to list the current ReadyBoost (requires USB 3.0) cache used by the Operating System, but also to display the logs of the memory pages managed by the store manager.

Parameter: /cache

```
Command
0: kd> !ms_store /cache
Cache @ 0xFFFFFA8007F9AC50
    CacheIndex: 0# Store Manager cache file size = 7593787392 bytes (7242 Mb) (7 Gb)
    Handle: 0xFFFFFFFF80001958
    FileObject: 0xFFFFFA800796D370 (more)
    ID: _??_USBSTOR#Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP#130315135026B024&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
```

Parameter: /log

```
Command
0: kd> !ms_store /log
  ID # Action    EPROCESS            Application Name  Page Count  Priority  Virtual Address Range
  ---- ------    ------------------  ----------------  ----------  --------  ------------------------------------
     0 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000056E2000-0x00000000056E3000
     1 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000056E4000-0x00000000056E5000
     2 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000056EF000-0x00000000056F0000
     3 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000005706000-0x0000000005707000
     4 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000005709000-0x000000000570A000
     5 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x000000000572E000-0x000000000572F000
     6 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000005784000-0x0000000005785000
     7 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000005785000-0x0000000005786000
     8 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x000000000578B000-0x000000000578C000
     9 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000005790000-0x0000000005791000
    10 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000005795000-0x0000000005796000
    11 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006E74000-0x0000000006E75000
    12 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006EC0000-0x0000000006EC1000
    13 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               2  P5        0x0000000006EC2000-0x0000000006EC4000
    14 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006EC4000-0x0000000006EC5000
    15 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006ECB000-0x0000000006ECC000
    16 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006EDB000-0x0000000006EDC000
    17 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006EDE000-0x0000000006EDF000
    18 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006EE2000-0x0000000006EE3000
    19 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006EE3000-0x0000000006EE4000
    20 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006EE4000-0x0000000006EE5000
    21 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006EE5000-0x0000000006EE6000
    22 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               3  P2        0x0000000006EE9000-0x0000000006EEC000
    23 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               2  P5        0x0000000006EED000-0x0000000006EEF000
    24 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006EF5000-0x0000000006EF6000
    25 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006F09000-0x0000000006F0A000
    26 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x0000000006F41000-0x0000000006F42000
    27 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x0000000006F4D000-0x0000000006F4E000
    28 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x00000000054B0000-0x00000000054B1000
    29 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000054B1000-0x00000000054B2000
    30 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x00000000054B3000-0x00000000054B4000
    31 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000054B4000-0x00000000054B5000
    32 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P5        0x00000000054B8000-0x00000000054B9000
    33 Add       0xFFFFFA8007BDA2A0  vcpkgsrv.exe               1  P2        0x00000000054C2000-0x00000000054C3000
```

!ms_drivers

!ms_drivers will go ahead and display a list of drivers that are currently loaded.

In this example, here's a few of the drivers loaded at the time of the crash in this kernel-dump:

```
5: kd> !ms_drivers
    | \Driver\fvevol                  | 0xfffff801c1200000 | 0x00095000 | \SystemRoot\System32\DRIVERS\fvevol.sys
    | \Driver\vdrvroot                 | 0xfffff801c09e6000 | 0x0000D000 | \SystemRoot\System32\drivers\vdrvroot.sys
    | \Driver\NetBT                    | 0xfffff801c1b59000 | 0x0004C000 | \SystemRoot\System32\DRIVERS\netbt.sys
    | \Driver\acpiex                   | 0xfffff801c074d000 | 0x00018000 | \SystemRoot\System32\Drivers\acpiex.sys
    | \Driver\Wdf01000                 | 0xfffff801c0600000 | 0x000CF000 | \SystemRoot\system32\drivers\Wdf01000.sys
    | \Driver\WdNisDrv                 | 0xfffff801c37cd000 | 0x00021000 | \SystemRoot\system32\Drivers\WdNisDrv.sys
    | \Driver\mpsdrv                   | 0xfffff801c3d4a000 | 0x00017000 | \SystemRoot\System32\drivers\mpsdrv.sys
    | \Driver\storahci                 | 0xfffff801c0ba9000 | 0x0001D000 | \SystemRoot\System32\drivers\storahci.sys
    | \Driver\pciide                   | 0xfffff801c0b09000 | 0x00008000 | \SystemRoot\System32\drivers\pciide.sys
    | \Driver\lltdio                   | 0xfffff801c37a1000 | 0x00014000 | \SystemRoot\system32\DRIVERS\lltdio.sys
    | \Driver\Psched                   | 0xfffff801c1d61000 | 0x0002A000 | \SystemRoot\system32\DRIVERS\pacer.sys
    | \Driver\BasicRender              | 0xfffff801c0cc9000 | 0x0000E000 | \SystemRoot\System32\drivers\BasicRender.sys
    | \Driver\disk                     | 0xfffff801c15ce000 | 0x0001C000 | \SystemRoot\System32\drivers\disk.sys
    | \Driver\HTTP                     | 0xfffff801c3c30000 | 0x000FA000 | \SystemRoot\system32\drivers\HTTP.sys
    | \Driver\LVRS64                   | 0xfffff801c3439000 | 0x00054000 | \SystemRoot\system32\DRIVERS\lvrs64.sys
    | \Driver\tunnel                   | 0xfffff801c4563000 | 0x0002D000 | \SystemRoot\system32\DRIVERS\tunnel.sys
    | \Driver\monitor                  | 0xfffff801c36d7000 | 0x0000E000 | \SystemRoot\System32\drivers\monitor.sys
    | \Driver\usbehci                  | 0xfffff801c2074000 | 0x00018000 | \SystemRoot\System32\drivers\usbehci.sys
    | \Driver\ahcache                  | 0xfffff801c1f8d000 | 0x00017000 | \SystemRoot\system32\DRIVERS\ahcache.sys
    | \Driver\pcw                      | 0xfffff801c1049000 | 0x00010000 | \SystemRoot\System32\drivers\pcw.sys
    | \Driver\CompFilter64             | 0xfffff801c378b000 | 0x00005000 | \SystemRoot\System32\drivers\lvbflt64.sys
    | \Driver\UCX01000                 | 0xfffff801c208c000 | 0x00032000 | \SystemRoot\System32\drivers\ucx01000.sys
    | \Driver\USBXHCI                  | 0xfffff801c1c70000 | 0x00055000 | \SystemRoot\System32\drivers\USBXHCI.SYS
    | \Driver\partmgr                  | 0xfffff801c081c000 | 0x00018000 | \SystemRoot\System32\drivers\partmgr.sys
    | \Driver\MsLldp                   | 0xfffff801c4590000 | 0x00016000 | \SystemRoot\system32\DRIVERS\mslldp.sys
    | \Driver\PEAUTH                   | 0xfffff801c429d000 | 0x000A9000 | \SystemRoot\system32\drivers\peauth.sys
    | \Driver\emupia                   | 0xfffff801c338f000 | 0x0004A000 | \SystemRoot\system32\drivers\emupia2k.sys
    | \Driver\e1cexpress               | 0xfffff801c2000000 | 0x00074000 | \SystemRoot\system32\DRIVERS\e1c64x64.sys
```

With this command, we can also view in-depth IRP information regarding a driver:

```
5: kd> !ms_drivers /object 0xFFFFE0016ED4E060
    | \Driver\e1cexpress               | 0xfffff801c2000000 | 0x00074000 | \SystemRoot\system32\DRIVERS\e1c64x64.sys
    \---| IRP_MJ_CREATE                  | 0xFFFFF801C1071AC0 |          | ndis!ndisCreateIrpHandler
    \---| IRP_MJ_CREATE_NAMED_PIPE       | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_CLOSE                   | 0xFFFFF801C107192C |          | ndis!ndisCloseIrpHandler
    \---| IRP_MJ_READ                    | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_WRITE                   | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_QUERY_INFORMATION       | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_SET_INFORMATION         | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_QUERY_EA                | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_SET_EA                  | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_FLUSH_BUFFERS           | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_QUERY_VOLUME_INFORMATION | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_SET_VOLUME_INFORMATION  | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_DIRECTORY_CONTROL       | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_FILE_SYSTEM_CONTROL     | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_DEVICE_CONTROL          | 0xFFFFF801C10F7DB0 |          | ndis!ndisDeviceControlIrpHandler
    \---| IRP_MJ_INTERNAL_DEVICE_CONTROL | 0xFFFFF801C10C4BC0 |          | ndis!ndisDeviceInternalIrpDispatch
    \---| IRP_MJ_SHUTDOWN                | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_LOCK_CONTROL            | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_CLEANUP                 | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_CREATE_MAILSLOT         | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_QUERY_SECURITY          | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_SET_SECURITY            | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_POWER                   | 0xFFFFF801C1084040 |          | ndis!ndisPowerDispatch
    \---| IRP_MJ_SYSTEM_CONTROL          | 0xFFFFF801C10FFB5C |          | ndis!ndisWMIDispatch
    \---| IRP_MJ_DEVICE_CHANGE           | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_QUERY_QUOTA             | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_SET_QUOTA               | 0xFFFFF801C10F85A0 |          | ndis!ndisDummyIrpHandler
    \---| IRP_MJ_PNP                     | 0xFFFFF801C10FFD34 |          | ndis!ndisPnPDispatch
```

In the above image we can see the driver-specific I/O stack location within e1cexpress.sys' IRP. Here we can see function codes such as IRP_MJ_CREATE which opens the target device object, indicating that it is present and available for I/O operations.

!ms_timers

```
5: kd> !ms_timers

    |--------------------------|-------------------|-------------------|---------|-------------------|-------------------------------------------------------|
    | Timer Type               | Timer             | Dpc               | Period  | Deferred Routine  | Hooked | Module |
    |--------------------------|-------------------|-------------------|---------|-------------------|-------------------------------------------------------|
    | TimerNotificationObject  | 0xFFFFE0016E0CC060 | 0xFFFFE0016E0CC100 |       0 | 0xFFFFF801AE38E6D8 |        | nt!ExpTimerDpcRoutine
    | TimerNotificationObject  | 0xFFFFF801AE578408 | 0x9267CD35C5BF2EB9 |       0 | 0x0000000000000000 |        |
    | TimerNotificationObject  | 0xFFFFF801AE538660 | 0xFFFFF801AE538620 |       0 | 0xFFFFF801AE4C1280 |        | nt!ExpNextYearDpcRoutine
    | TimerNotificationObject  | 0xFFFFF801AE578608 | 0xAB65CD35C5F72BE6 |       0 | 0x0000000000000000 |        |
    | TimerNotificationObject  | 0xFFFFF801C097D7E0 | 0xFFFFF801C097D840 |       0 | 0xFFFFF801C0909550 |        | cng!reseedDpcRoutine
    | TimerNotificationObject  | 0xFFFFE001706E5180 | 0x0000000000000000 |       0 | 0x0000000000000000 |        |
```

!ms_timers displays the KTIMER structure, which is an opaque structure that represents and contains various timer objects. This command can be helpful to figure out what drivers created what timer objects, what drivers called what routines, etc.

!ms_gdt

```
6: kd> !ms_gdt
    |-----|-----|--------------------|-------------------|
    | Cre | Idx | Type               | Address           | Name
    |-----|-----|--------------------|-------------------|
    |   0 |   0 | Data RO            | 0x0000000000000000 | None
    |   0 |   1 | TSS32 Busy         | 0x0000FFFF00000000 | None
    |   0 |   2 | TSS32 Busy         | 0x0000FFFF00000000 | None
    |   0 |   3 | TSS32 Busy         | 0x0000000000000000 | None
    |   0 |   4 | Code RE Ac         | 0xFFFFFFFFAFCC2080 | None
    |   0 |   5 | TSS16 Busy         | 0xFFFFFFFFFFC67000 | None
    |   0 |   6 | TSS32 Busy         | 0x0000000000000000 | None
    |   0 |   7 | Data RO            | 0x0000000000000000 | None
    |   0 |   8 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   9 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   a | Code RE C          | 0xFFFFFFFFAE030010 | None
    |   0 |   b | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   c | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   d | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   e | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |   f | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  10 | Code RE C          | 0xFFFFFFFFAE010010 | None
    |   0 |  11 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  12 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  13 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  14 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  15 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  16 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  17 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  18 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  19 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  1a | Code RE C          | 0xFFFFFFFFAE020010 | None
    |   0 |  1b | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  1c | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  1d | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  1e | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  1f | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  20 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  21 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  22 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  23 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  24 | Code RE C          | 0xFFFFFFFFAE000010 | None
    |   0 |  25 | Code RE C          | 0xFFFFFFFFAE000010 | None
```

!ms_gdt displays the Global Descriptor Table. Note on x64 that every selector is flat (0x0000000000000000 to 0xFFFFFFFFFFFFFFFF). This command can be extra helpful to check for any suspected hooking of the GDT, as attempting to do so on x64 will call a bug check. This is because x64 forbids hooking of the GDT.

!ms_idt

!ms_idt displays the Interrupt descriptor table. Very much like the GDT, if the IDT is hooked on an x64 system, it will call a bug check. This is due to the fact that Microsoft implemented (programmatically) a prevention of hooking the IDT with a kernel-mode driver that would normally intercept calls to the IDT and then add in its own processing. This is why in the above image, there is 'No' as far as the eye can see.

```
Command
16.kd:x86> !ms_idt
    |-----|-----|--------------------|-------------------------------------------------------|---------|--------|
    | Cre | Idx | Address            | Name                                                  | Patched | Hooked |
    |-----|-----|--------------------|-------------------------------------------------------|---------|--------|
    |   0 |   0 | 0xFFFFF80002674C40 | nt!KiDivideErrorFault                                 |         | No     |
    |   0 |   1 | 0xFFFFF80002674D40 | nt!KiDebugTrapOrFault                                 |         | No     |
    |   0 |   2 | 0xFFFFF80002674F00 | nt!KiNmiInterrupt                                     |         | No     |
    |   0 |   3 | 0xFFFFF80002675280 | nt!KiBreakpointTrap                                   |         | No     |
    |   0 |   4 | 0xFFFFF80002675380 | nt!KiOverflowTrap                                     |         | No     |
    |   0 |   5 | 0xFFFFF80002675480 | nt!KiBoundFault                                       |         | No     |
    |   0 |   6 | 0xFFFFF80002675580 | nt!KiInvalidOpcodeFault                               |         | No     |
    |   0 |   7 | 0xFFFFF800026757C0 | nt!KiNpxNotAvailableFault                             |         | No     |
    |   0 |   8 | 0xFFFFF80002675880 | nt!KiDoubleFaultAbort                                 |         | No     |
    |   0 |   9 | 0xFFFFF80002675940 | nt!KiNpxSegmentOverrunAbort                           |         | No     |
    |   0 |  10 | 0xFFFFF80002675A00 | nt!KiInvalidTssFault                                  |         | No     |
    |   0 |  11 | 0xFFFFF80002675AC0 | nt!KiSegmentNotPresentFault                           |         | No     |
    |   0 |  12 | 0xFFFFF80002675C00 | nt!KiStackFault                                       |         | No     |
    |   0 |  13 | 0xFFFFF80002675D40 | nt!KiGeneralProtectionFault                           |         | No     |
    |   0 |  14 | 0xFFFFF80002675E80 | nt!KiPageFault                                        |         | No     |
    |   0 |  15 | 0xFFFFF800027AC0F0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  16 | 0xFFFFF80002676240 | nt!KiFloatingErrorFault                               |         | No     |
    |   0 |  17 | 0xFFFFF800026763C0 | nt!KiAlignmentFault                                   |         | No     |
    |   0 |  18 | 0xFFFFF800026764C0 | nt!KiMcheckAbort                                      |         | No     |
    |   0 |  19 | 0xFFFFF80002676840 | nt!KiXmmException                                     |         | No     |
    |   0 |  20 | 0xFFFFF800027AC140 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  21 | 0xFFFFF800027AC150 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  22 | 0xFFFFF800027AC160 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  23 | 0xFFFFF800027AC170 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  24 | 0xFFFFF800027AC180 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  25 | 0xFFFFF800027AC190 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  26 | 0xFFFFF800027AC1A0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  27 | 0xFFFFF800027AC1B0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  28 | 0xFFFFF800027AC1C0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  29 | 0xFFFFF800027AC1D0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  30 | 0xFFFFF800027AC1E0 | nt!KxUnexpectedInterrupt0                             |         | No     |
    |   0 |  31 | 0xFFFFF80002654C10 | nt!KiApcInterrupt                                     |         | No     |
    |   0 |  32 | 0xFFFFF800027AC200 | nt!KxUnexpectedInterrupt0                             |         | No     |
```

!ms_hivelist

```
6: kd> !ms_hivelist

    |-----------------------|-------------------------------------------------------------------------|-----------------------|
    | Hive ('U' = Untrusted) | Hive Root Path                                                          | File user name                |
    |-----------------------|-------------------------------------------------------------------------|-----------------------|
    | 0xFFFFC000B7028000 (T) | \REGISTRY\MACHINE\SYSTEM                                                |                               |
    | 0xFFFFC000B7039000 (T) | \REGISTRY\MACHINE\HARDWARE                                              |                               |
    | 0xFFFFC000B8363000 (U) | \REGISTRY\MACHINE\BCD00000000                                           | \Device\HarddiskVolume1\Boot\BCD |
    | 0xFFFFC000B8382000 (T) | \REGISTRY\MACHINE\SOFTWARE                                              | \SystemRoot\System32\Config\SOFTWARE |
    | 0xFFFFC000B8F9D000 (U) | \REGISTRY\USER\.DEFAULT                                                 | \SystemRoot\System32\Config\DEFAULT |
    | 0xFFFFC000B8910000 (T) | \REGISTRY\MACHINE\SECURITY                                              | \SystemRoot\System32\Config\SECURITY |
    | 0xFFFFC000B898A000 (T) | \REGISTRY\MACHINE\SAM                                                   | \SystemRoot\System32\Config\SAM |
    | 0xFFFFC000B8A75000 (U) | \REGISTRY\USER\S-1-5-20                                                 | \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT |
    | 0xFFFFC000B8B77000 (U) | \REGISTRY\USER\S-1-5-19                                                 | \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT |
    | 0xFFFFC000B95FD000 (U) | \Registry\User\S-1-5-21-413046472-550950853-4173456331-1001             | \??\C:\Users\Patrick\ntuser.dat |
    | 0xFFFFC000BA3DA000 (U) | \Registry\User\S-1-5-21-413046472-550950853-4173456331-1001_Classes     | \??\C:\Users\Patrick\AppData\Local\Microsoft\Windows\UsrClass.dat |
```

!ms_hivelist displays a list of registry hives.

We can look directly into a hive (\Registry\Machine\Software for example) to see its subkeys, values, etc:

```
6: kd> !reg openkeys 0xFFFFC000B8382000

Hive: \REGISTRY\MACHINE\SOFTWARE
=================================================================================
Index 0:        d780b327 kcb=ffffc000b9400948 cell=010b9608 f=00200001 \REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIPTIONS\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4
                c3d28eb3 kcb=ffffc000b8881948 cell=00095630 f=00200004 \REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{1CF1260C-4DD0-4EBB-811F-33C572699FDE}
Index 2:        a2b3d7a2 kcb=ffffc000b910fcc0 cell=00a59ee9 f=00200010 \REGISTRY\MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\OID\ENCODINGTYPE 0\CRYPTDLLDECODEOBJECTEX
                737b9d19 kcb=ffffc000bba84948 cell=019f64f0 f=00200000 \REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\NETWORKLIST\DEFAULTMEDIACOST
                b4448991 kcb=ffffc000b9bd9258 cell=005d70d8 f=00200000 \REGISTRY\MACHINE\SOFTWARE\CLASSES\UNMARSHALERS\SYSTEM
Index 3:        8b6f5641 kcb=ffffc000ba175b98 cell=00a6fb28 f=00200002 \REGISTRY\MACHINE\SOFTWARE\MICROSOFT\CTF\TIP\{78CB5B0E-26ED-4FCC-854C-77E8F3D1AA80}
```

!ms_exqueue

!exqueue doesn't work properly on Windows 8, so a working version needed to be implemented. Just like the original command this one dispaly the working threads queue.

```
Command

0: kd> !ms_exqueue
ExpWorkerThreadBalanceManager = 0xFFFFFFFF85490040

**** NUMA Node 0 CriticalWorkQueue
THREAD 0xFFFFFFFF85475040 Cid 0004.0024 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF85434AC0 Cid 0004.002C Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF854A0B40 Cid 0004.0020 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF85486BC0 Cid 0004.0028 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF854AB040 Cid 0004.0030 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF86C1F6C0 Cid 0004.08B4 Teb: 0x0 Win32Thread: 0x0

**** NUMA Node 0 DelayedWorkQueue
THREAD 0xFFFFFFFF86FFFA00 Cid 0004.00DC Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF854AB880 Cid 0004.0720 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF8548A040 Cid 0004.0514 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF856E8700 Cid 0004.0F84 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF88970640 Cid 0004.09C8 Teb: 0x0 Win32Thread: 0x0

**** NUMA Node 0 HyperCriticalWorkQueue
THREAD 0xFFFFFFFF863B1040 Cid 0004.00F0 Teb: 0x0 Win32Thread: 0x0

**** NUMA Node 0 NormalWorkQueue
THREAD 0xFFFFFFFF889B5C80 Cid 0004.0910 Teb: 0x0 Win32Thread: 0x0
THREAD 0xFFFFFFFF856C1740 Cid 0004.0918 Teb: 0x0 Win32Thread: 0x0

**** NUMA Node 0 BackgroundWorkQueue
THREAD 0xFFFFFFFF85472B80 Cid 0004.0864 Teb: 0x0 Win32Thread: 0x0

**** NUMA Node 0 RealTimeWorkQueue

**** NUMA Node 0 SuperCriticalWorkQueue
```