Becoming independent

Introduction to Windbg

Assembly language programming
By xorpd

xorpd.net

Windbg

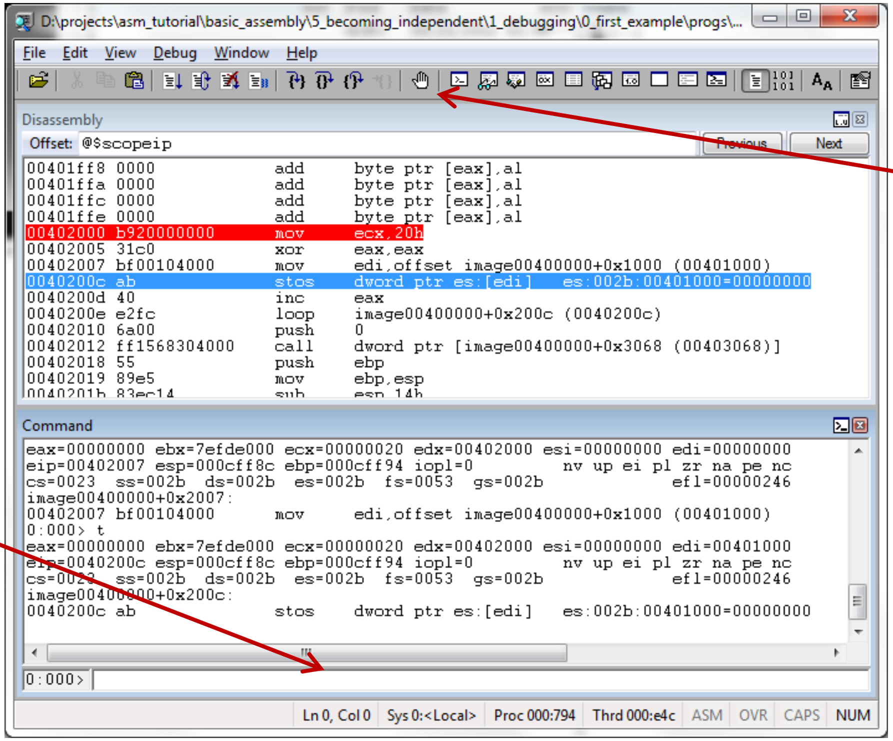
- A debugger for the Windows operation systems.
  - Works on every windows version.
- Developed by Microsoft Corporation.
  - And used by Microsoft developers.
- Can be downloaded **for free** from Microsoft’s website.
- A very powerful debugger.

Main features

- Basic debugging features:
  - Stepping.
  - Software Breakpoints.
  - Hardware breakpoints.
- Extendable (Extension DLLs)
- Supports debugging symbols.
- Kernel mode debugging.
  - Can be used to debug the operation system.
- Analysis of crash dumps.

Interface

- Windbg has both GUI and command line interfaces.
  - Some basic commands could be executed from the GUI.
  - For more advanced commands, the command line is necessary.


D:\projects\asm_tutorial\basic_assembly\5_becoming_independent\1_debugging\0_first_example\progs\...
File
Edit
View
Debug
Window
Help
Disassembly
Offset:
Previous
Next
Command

Offset: @$scopeip

```
00401ff8 0000            add     byte ptr [eax],al
00401ffa 0000            add     byte ptr [eax],al
00401ffc 0000            add     byte ptr [eax],al
00401ffe 0000            add     byte ptr [eax],al
00402000 b920000000      mov     ecx,20h
00402005 31c0            xor     eax,eax
00402007 bf00104000      mov     edi,offset image00400000+0x1000 (00401000)
0040200c ab              stos    dword ptr es:[edi]   es:002b:00401000=00000000
0040200d 40              inc     eax
0040200e e2fc            loop    image00400000+0x200c (0040200c)
00402010 6a00            push    0
00402012 ff1568304000    call    dword ptr [image00400000+0x3068 (00403068)]
00402018 55              push    ebp
00402019 89e5            mov     ebp,esp
0040201b 83ec14          sub     esp,14h
```

```
eax=00000000 ebx=7efde000 ecx=00000020 edx=00402000 esi=00000000 edi=00000000
eip=00402007 esp=000cff8c ebp=000cff94 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
image00400000+0x2007:
00402007 bf00104000      mov     edi,offset image00400000+0x1000 (00401000)
0:000> t
eax=00000000 ebx=7efde000 ecx=00000020 edx=00402000 esi=00000000 edi=00401000
eip=0040200c esp=000cff8c ebp=000cff94 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
image00400000+0x200c:
0040200c ab              stos    dword ptr es:[edi]   es:002b:00401000=00000000
```

```
0:000>
```

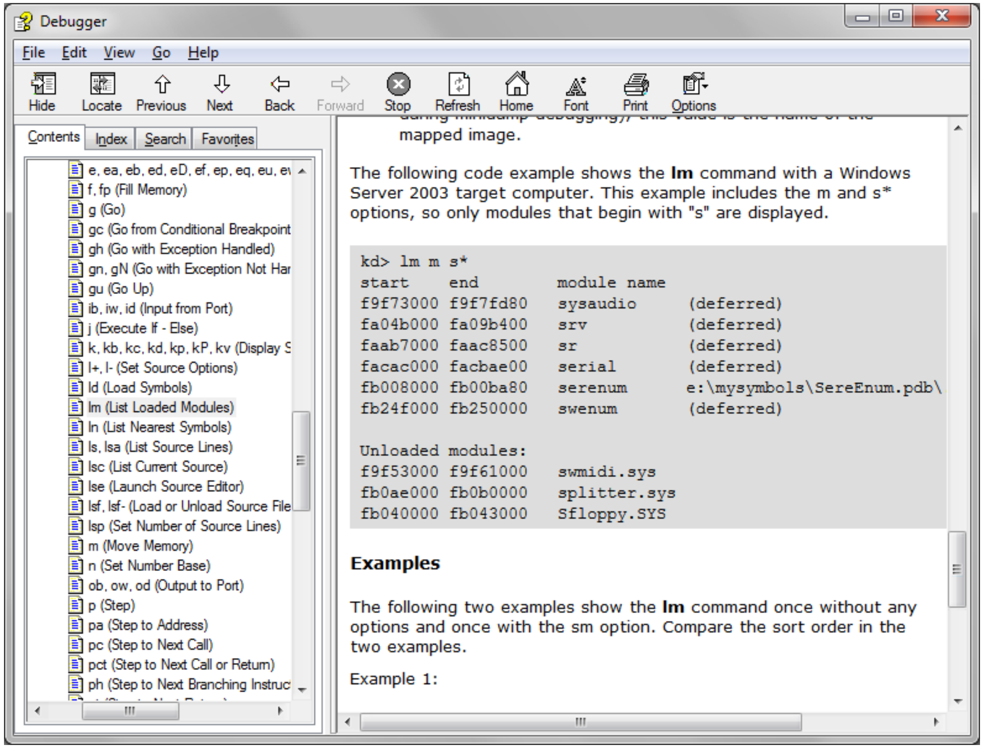
Ln 0, Col 0 Sys 0:<Local> Proc 000:794 Thrd 000:e4c ASM OVR CAPS NUM

GUI

Command line

Windbg Help

- Windbg has very extensive documentation.
- Could be found in help -> contents


Debugger
File
Edit
View
Go
Help
Hide
Locate
Previous
Next
Back
Forward
Stop
Refresh
Home
Font
Print
Options
Contents
Index
Search
Favorites
e, ea, eb, ed, eD, ef, ep, eq, eu, ew
f, fp (Fill Memory)
g (Go)
gc (Go from Conditional Breakpoint
gh (Go with Exception Handled)
gn, gN (Go with Exception Not Har
gu (Go Up)
ib, iw, id (Input from Port)
j (Execute If - Else)
k, kb, kc, kd, kp, kP, kv (Display S
l+, l- (Set Source Options)
ld (Load Symbols)
lm (List Loaded Modules)
ln (List Nearest Symbols)
ls, lsa (List Source Lines)
lsc (List Current Source)
lse (Launch Source Editor)
lsf, lsf- (Load or Unload Source File
lsp (Set Number of Source Lines)
m (Move Memory)
n (Set Number Base)
ob, ow, od (Output to Port)
p (Step)
pa (Step to Address)
pc (Step to Next Call)
pct (Step to Next Call or Return)
ph (Step to Next Branching Instruc

mapped image.

The following code example shows the **lm** command with a Windows Server 2003 target computer. This example includes the m and s* options, so only modules that begin with "s" are displayed.

```
kd> lm m s*
start    end        module name
f9f73000 f9f7fd80   sysaudio     (deferred)
fa04b000 fa09b400   srv          (deferred)
faab7000 faac8500   sr           (deferred)
facac000 facbae00   serial       (deferred)
fb008000 fb00ba80   serenum      e:\mysymbols\SereEnum.pdb\
fb24f000 fb250000   swenum       (deferred)

Unloaded modules:
f9f53000 f9f61000   swmidi.sys
fb0ae000 fb0b0000   splitter.sys
fb040000 fb043000   Sfloppy.SYS
```

Examples

The following two examples show the **lm** command once without any options and once with the sm option. Compare the sort order in the two examples.

Example 1: