Reverse engineering

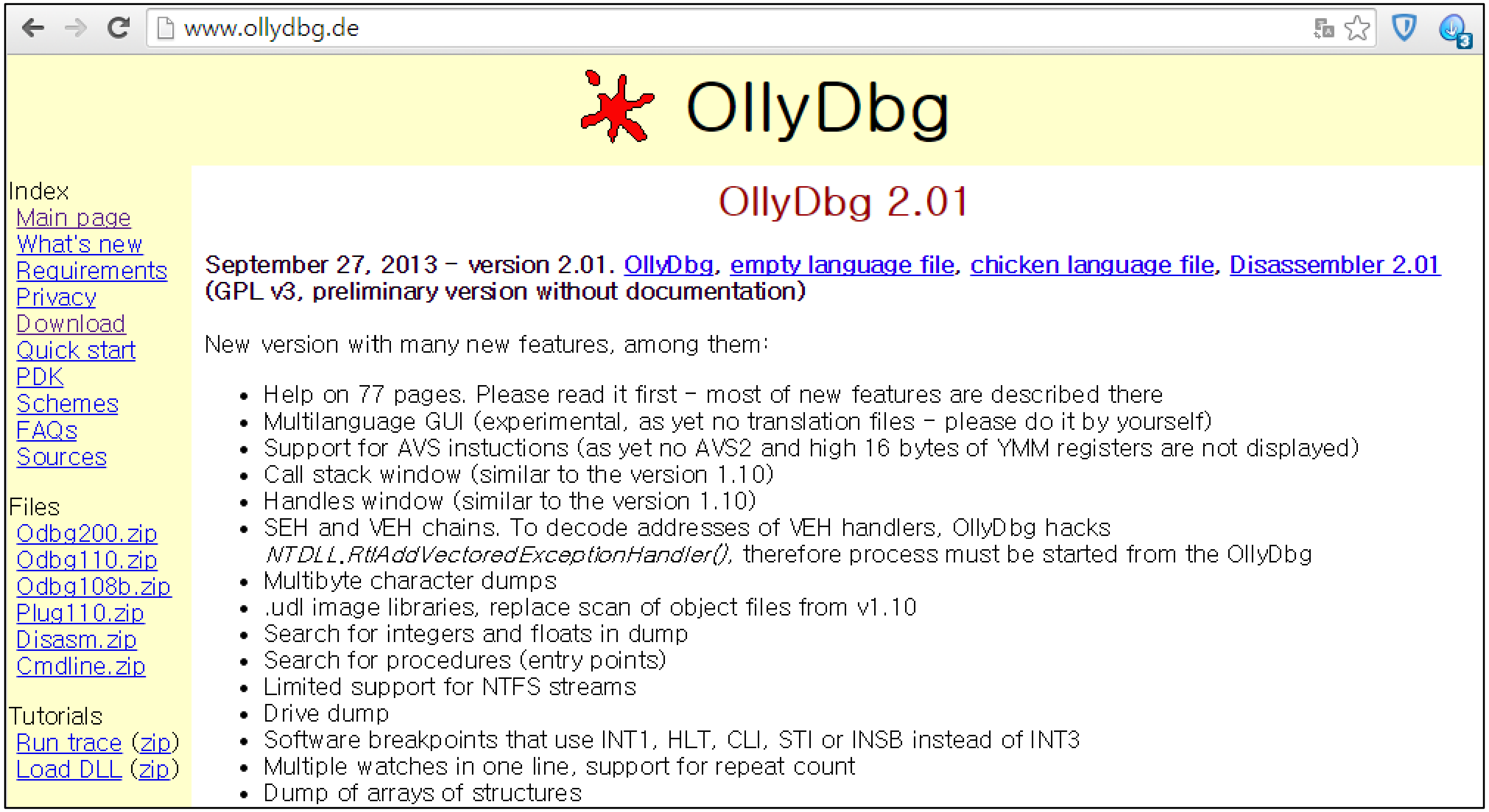
OllyDbg

Chanung Pak

koha@korea.ac.kr

OllyDbg

- **OllyDbg v2.01(27-Sep-2013)**
- **Progress inOllyDbg 64(05-Feb-2014)**



Index
Main page
What's new
Requirements
Privacy
Download
Quick start
PDK
Schemes
FAQs
Sources

Files
Odbg200.zip
Odbg110.zip
Odbg108b.zip
Plug110.zip
Disasm.zip
Cmdline.zip

Tutorials
Run trace (zip)
Load DLL (zip)

OllyDbg 2.01

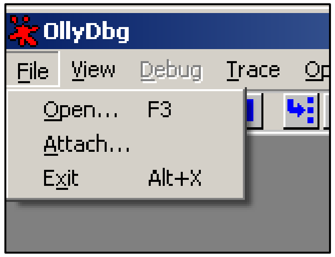
September 27, 2013 - version 2.01. OllyDbg, empty language file, chicken language file, Disassembler 2.01 (GPL v3, preliminary version without documentation)

New version with many new features, among them:

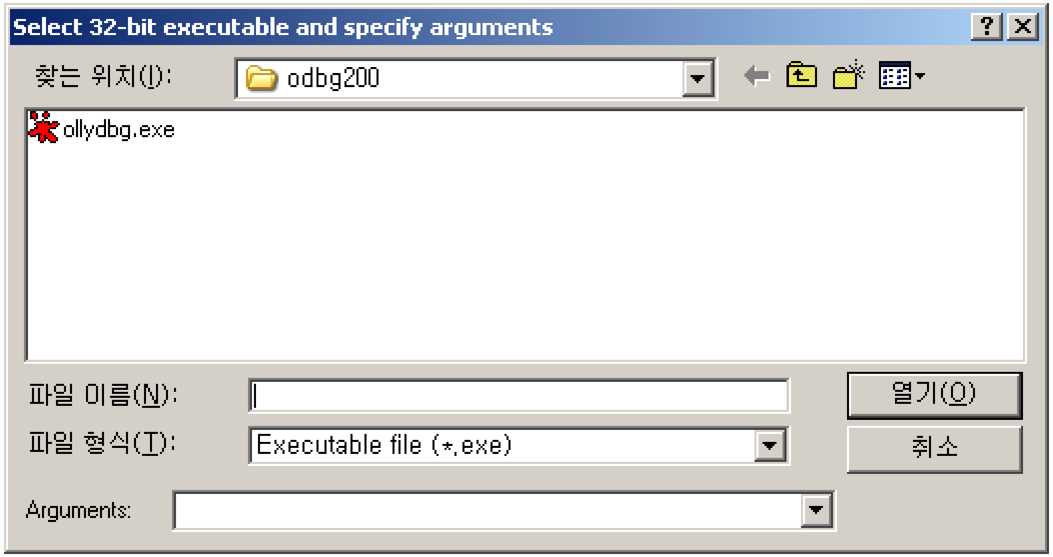
- Help on 77 pages. Please read it first - most of new features are described there
- Multilanguage GUI (experimental, as yet no translation files - please do it by yourself)
- Support for AVS instuctions (as yet no AVS2 and high 16 bytes of YMM registers are not displayed)
- Call stack window (similar to the version 1.10)
- Handles window (similar to the version 1.10)
- SEH and VEH chains. To decode addresses of VEH handlers, OllyDbg hacks *NTDLL.RtlAddVectoredExceptionHandler()*, therefore process must be started from the OllyDbg
- Multibyte character dumps
- .udl image libraries, replace scan of object files from v1.10
- Search for integers and floats in dump
- Search for procedures (entry points)
- Limited support for NTFS streams
- Drive dump
- Software breakpoints that use INT1, HLT, CLI, STI or INSB instead of INT3
- Multiple watches in one line, support for repeat count
- Dump of arrays of structures

OllyDbg

- **Launching the Debugger**



  - Open -‘F3’


Select 32-bit executable and specify arguments

찾는 위치(I): odbg200

ollydbg.exe

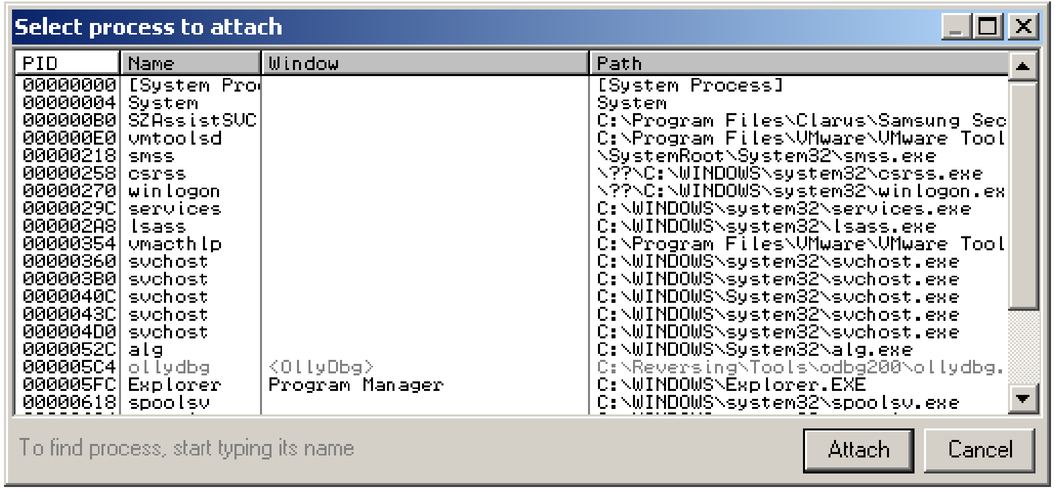
파일 이름(N):

파일 형식(T): Executable file (*.exe)

Arguments:

  - Set new arguments

  - Attach

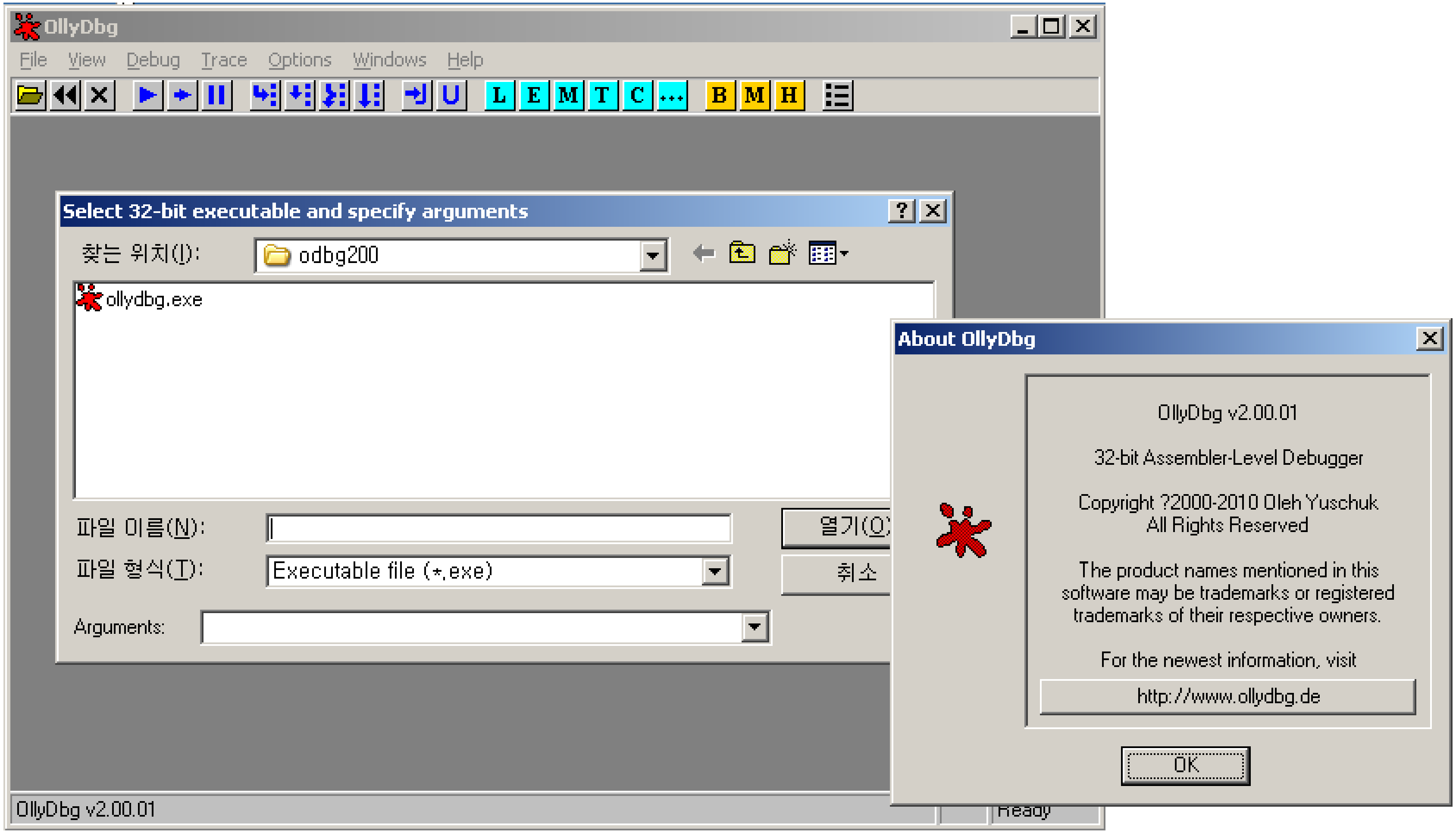

Select process to attach

PID	Name	Window	Path
00000000	[System Pro		[System Process]
00000004	System		System
000000B0	SZAssistSVC		C:\Program Files\Clarus\Samsung Sec
000000E0	vmtoolsd		C:\Program Files\VMware\VMware Tool
00000218	smss		\SystemRoot\System32\smss.exe
00000258	csrss		\??\C:\WINDOWS\system32\csrss.exe
00000270	winlogon		\??\C:\WINDOWS\system32\winlogon.ex
0000029C	services		C:\WINDOWS\system32\services.exe
000002A8	lsass		C:\WINDOWS\system32\lsass.exe
00000354	vmacthlp		C:\Program Files\VMware\VMware Tool
00000360	svchost		C:\WINDOWS\system32\svchost.exe
000003B0	svchost		C:\WINDOWS\system32\svchost.exe
0000040C	svchost		C:\WINDOWS\System32\svchost.exe
0000043C	svchost		C:\WINDOWS\system32\svchost.exe
000004D0	svchost		C:\WINDOWS\system32\svchost.exe
0000052C	alg		C:\WINDOWS\System32\alg.exe
000005C4	ollydbg	<OllyDbg>	C:\Reversing\Tools\odbg200\ollydbg.
000005FC	Explorer	Program Manager	C:\WINDOWS\Explorer.EXE
00000618	spoolsv		C:\WINDOWS\system32\spoolsv.exe

To find process, start typing its name

OllyDbg

- **Launching the Debugger**



OllyDbg
File View Debug Trace Options Windows Help
L E M T C ... B M H
Select 32-bit executable and specify arguments
ollydbg.exe
열기(O)
취소
About OllyDbg
OK
Ready

찾는 위치(I): odbg200

파일 이름(N):

파일 형식(T): Executable file (*.exe)

Arguments:

OllyDbg v2.00.01

32-bit Assembler-Level Debugger

Copyright ?2000-2010 Oleh Yuschuk
All Rights Reserved

The product names mentioned in this software may be trademarks or registered trademarks of their respective owners.

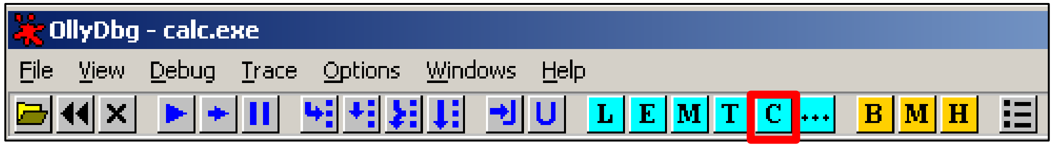
For the newest information, visit

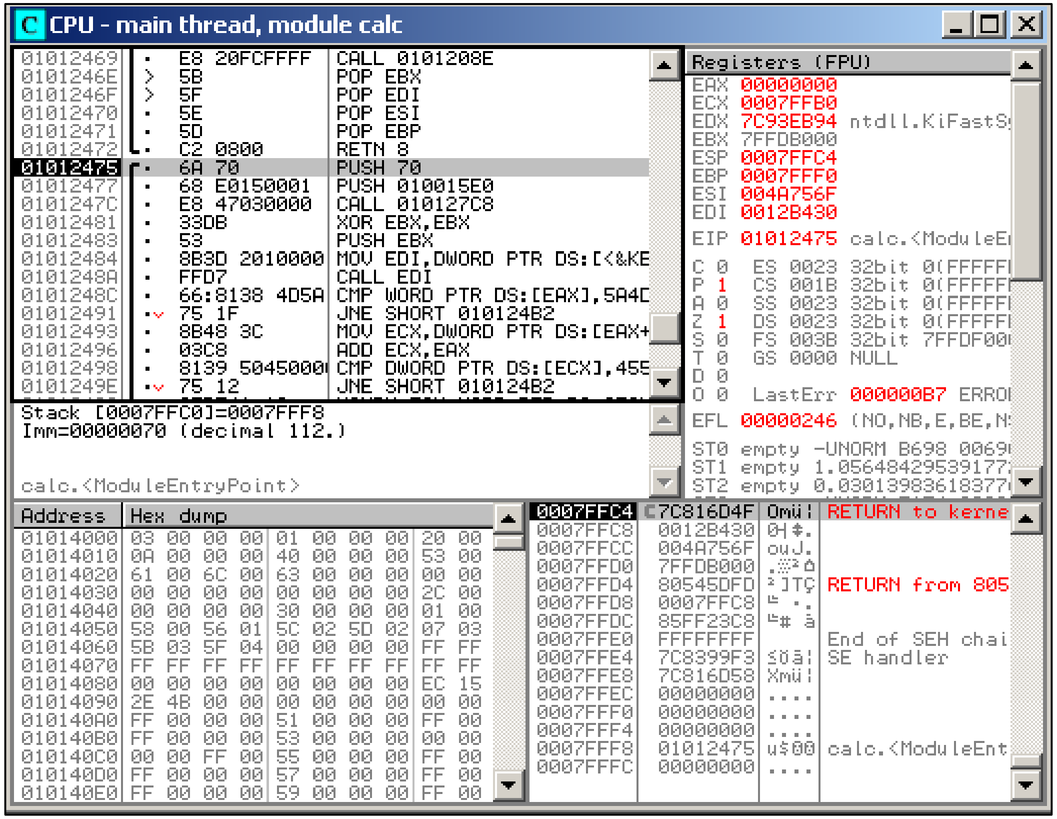
http://www.ollydbg.de

OllyDbg v2.00.01

OllyDbg

- **CPU View -'Alt + C'**





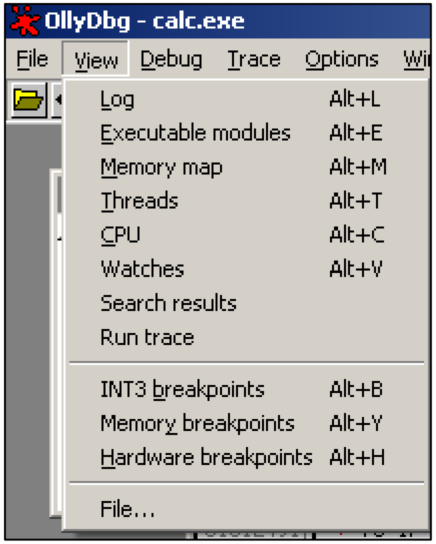
```
01012469  .   E8 20FCFFFF    CALL 0101208E
0101246E  >   5B             POP EBX
0101246F  >   5F             POP EDI
01012470  .   5E             POP ESI
01012471  .   5D             POP EBP
01012472  .   C2 0800        RETN 8
01012475  .   6A 70          PUSH 70
01012477  .   68 E0150001    PUSH 010015E0
0101247C  .   E8 47030000    CALL 010127C8
01012481  .   33DB           XOR EBX,EBX
01012483  .   53             PUSH EBX
01012484  .   8B3D 2010000   MOV EDI,DWORD PTR DS:[<&KE
0101248A  .   FFD7           CALL EDI
0101248C  .   66:8138 4D5A   CMP WORD PTR DS:[EAX],5A4D
01012491  .v  75 1F          JNE SHORT 010124B2
01012493  .   8B48 3C        MOV ECX,DWORD PTR DS:[EAX+
01012496  .   03C8           ADD ECX,EAX
01012498  .   8139 5045000   CMP DWORD PTR DS:[ECX],455
0101249E  .v  75 12          JNE SHORT 010124B2
```

```
Stack [0007FFC0]=0007FFF8
Imm=00000070 (decimal 112.)

calc.<ModuleEntryPoint>
```

```
Registers (FPU)
EAX 00000000
ECX 0007FFB0
EDX 7C93EB94 ntdll.KiFastS
EBX 7FFDB000
ESP 0007FFC4
EBP 0007FFF0
ESI 004A756F
EDI 0012B430

EIP 01012475 calc.<ModuleE

C 0  ES 0023 32bit 0(FFFFF
P 1  CS 001B 32bit 0(FFFFF
A 0  SS 0023 32bit 0(FFFFF
Z 1  DS 0023 32bit 0(FFFFF
S 0  FS 003B 32bit 7FFDF00
T 0  GS 0000 NULL
D 0
O 0  LastErr 000000B7 ERRO

EFL 00000246 (NO,NB,E,BE,N

ST0 empty -UNORM B698 0069
ST1 empty 1.0564842953917
ST2 empty 0.030139836183776
```

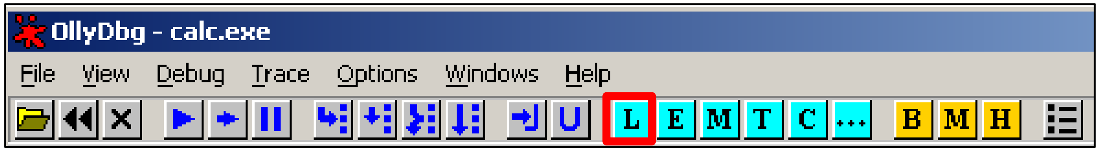
```
Address   Hex dump
01014000  03 00 00 00 01 00 00 00 20 00
01014010  0A 00 00 00 40 00 00 00 53 00
01014020  61 00 6C 00 63 00 00 00 00 00
01014030  00 00 00 00 00 00 00 00 2C 00
01014040  00 00 00 00 30 00 00 00 01 00
01014050  58 00 56 01 5C 02 5D 02 07 03
01014060  5B 03 5F 04 00 00 00 00 FF FF
01014070  FF FF FF FF FF FF FF FF FF FF
01014080  00 00 00 00 00 00 00 00 EC 15
01014090  2E 4B 00 00 00 00 00 00 00 00
010140A0  FF 00 00 00 51 00 00 00 FF 00
010140B0  FF 00 00 00 53 00 00 00 00 00
010140C0  00 00 FF 00 55 00 00 00 FF 00
010140D0  FF 00 00 00 57 00 00 00 FF 00
010140E0  FF 00 00 00 59 00 00 00 FF 00
```

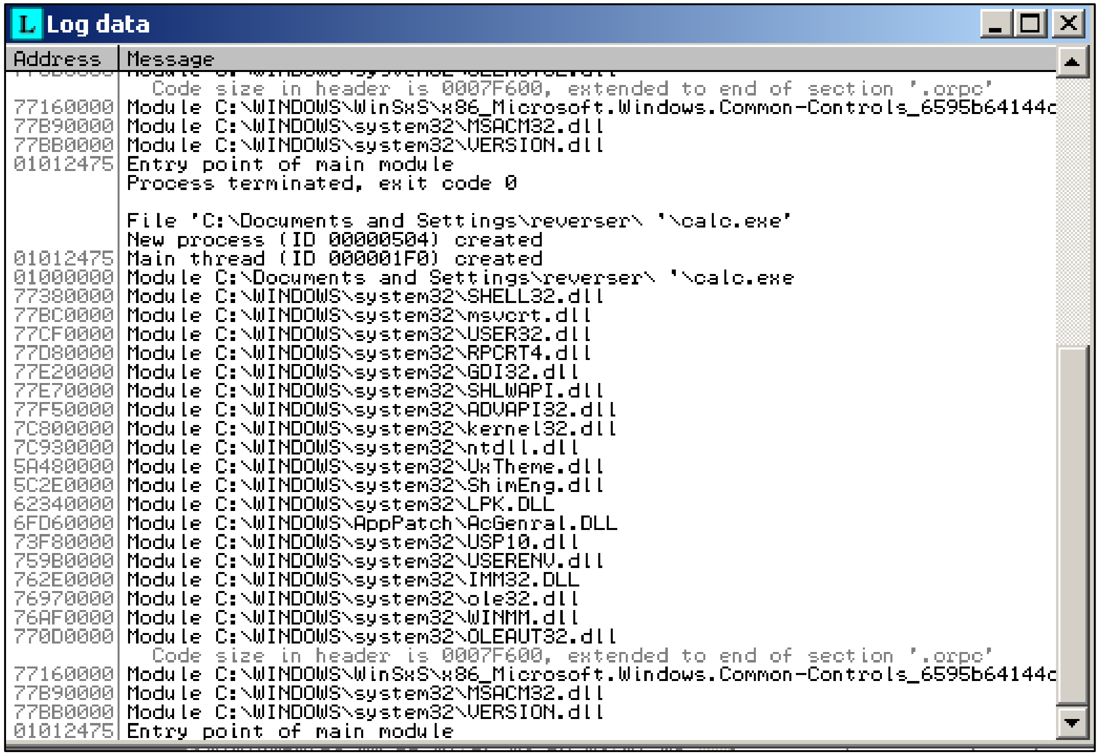
```
0007FFC4  7C816D4F  Omü¦  RETURN to kerne
0007FFC8  0012B430  0H‡.
0007FFCC  004A756F  ouJ.
0007FFD0  7FFDB000  .░²⌂
0007FFD4  80545DFD  ²]TÇ  RETURN from 805
0007FFD8  0007FFC8  ╚ •.
0007FFDC  85FF23C8  ╚# à
0007FFE0  FFFFFFFF        End of SEH chai
0007FFE4  7C8399F3  ≤Öâ¦  SE handler
0007FFE8  7C816D58  Xmü¦
0007FFEC  00000000  ....
0007FFF0  00000000  ....
0007FFF4  00000000  ....
0007FFF8  01012475  u$00  calc.<ModuleEnt
0007FFFC  00000000  ....
```



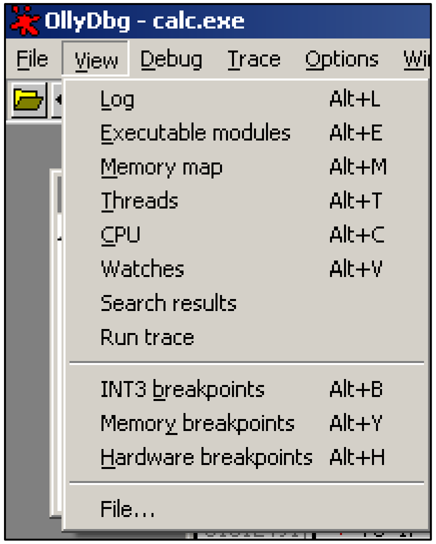
OllyDbg

- **Log View -‘Alt + L’**



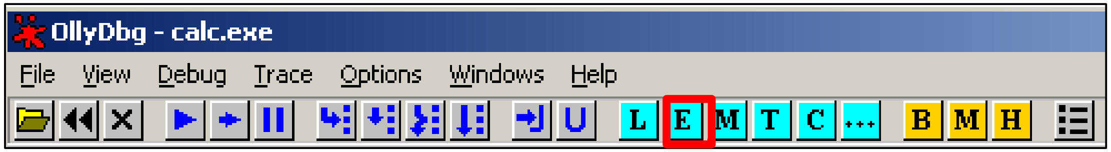


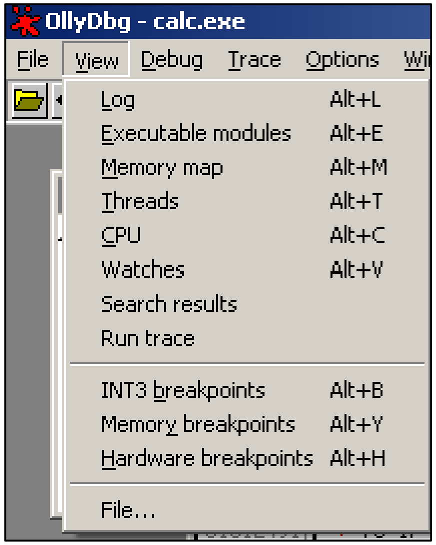
```
Address   Message
            Code size in header is 0007F600, extended to end of section '.orpc'
77160000 Module C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144c
77B90000 Module C:\WINDOWS\system32\MSACM32.dll
77BB0000 Module C:\WINDOWS\system32\VERSION.dll
01012475 Entry point of main module
         Process terminated, exit code 0

         File 'C:\Documents and Settings\reverser\ '\calc.exe'
         New process (ID 00000504) created
01012475 Main thread (ID 000001F0) created
01000000 Module C:\Documents and Settings\reverser\ '\calc.exe
77380000 Module C:\WINDOWS\system32\SHELL32.dll
77BC0000 Module C:\WINDOWS\system32\msvcrt.dll
77CF0000 Module C:\WINDOWS\system32\USER32.dll
77D80000 Module C:\WINDOWS\system32\RPCRT4.dll
77E20000 Module C:\WINDOWS\system32\GDI32.dll
77E70000 Module C:\WINDOWS\system32\SHLWAPI.dll
77F50000 Module C:\WINDOWS\system32\ADVAPI32.dll
7C800000 Module C:\WINDOWS\system32\kernel32.dll
7C930000 Module C:\WINDOWS\system32\ntdll.dll
5A480000 Module C:\WINDOWS\system32\UxTheme.dll
5C2E0000 Module C:\WINDOWS\system32\ShimEng.dll
62340000 Module C:\WINDOWS\system32\LPK.DLL
6FD60000 Module C:\WINDOWS\AppPatch\AcGenral.DLL
73F80000 Module C:\WINDOWS\system32\USP10.dll
759B0000 Module C:\WINDOWS\system32\USERENV.dll
762E0000 Module C:\WINDOWS\system32\IMM32.DLL
76970000 Module C:\WINDOWS\system32\ole32.dll
76AF0000 Module C:\WINDOWS\system32\WINMM.dll
770D0000 Module C:\WINDOWS\system32\OLEAUT32.dll
            Code size in header is 0007F600, extended to end of section '.orpc'
77160000 Module C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144c
77B90000 Module C:\WINDOWS\system32\MSACM32.dll
77BB0000 Module C:\WINDOWS\system32\VERSION.dll
01012475 Entry point of main module
```



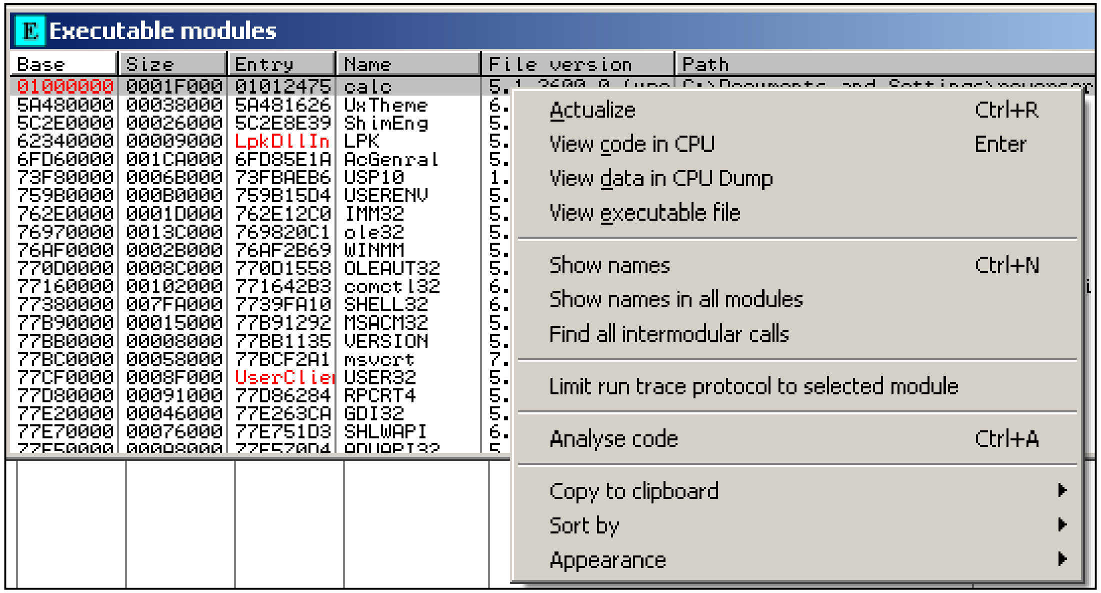
OllyDbg

- **Executable Modules View -‘Alt + E’**





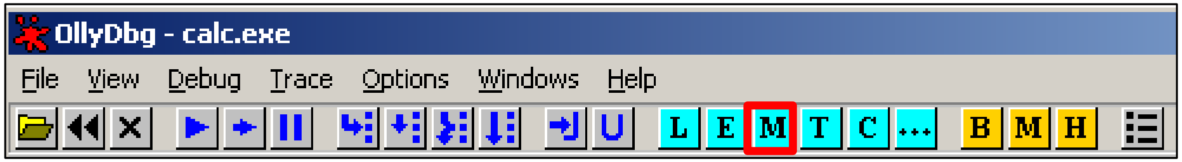
  - Names -‘Ctrl + N’

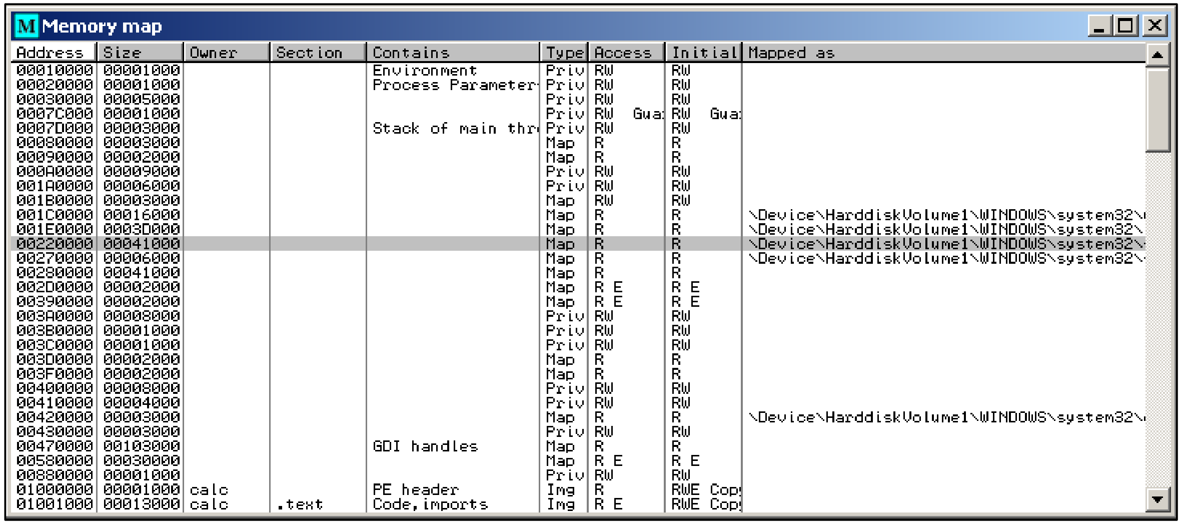


Base	Size	Entry	Name	File version	Path
01000000	0001F000	01012475	calc	5.1.2600.0 (xpsp	C:\Documents and Settings\
5A480000	00038000	5A481626	UxTheme	6.	
5C2E0000	00026000	5C2E8E39	ShimEng	5.	
62340000	00009000	LpkDllIn	LPK	5.	
6FD60000	001CA000	6FD85E1A	AcGenral	5.	
73F80000	0006B000	73FBAEB6	USP10	1.	
759B0000	000B0000	759B15D4	USERENV	5.	
762E0000	0001D000	762E12C0	IMM32	5.	
76970000	0013C000	769820C1	ole32	5.	
76AF0000	0002B000	76AF2B69	WINMM	5.	
770D0000	0008C000	770D1558	OLEAUT32	5.	
77160000	00102000	771642B3	comctl32	6.	
77380000	007FA000	7739FA10	SHELL32	6.	
77B90000	00015000	77B91292	MSACM32	5.	
77BB0000	00008000	77BB1135	VERSION	5.	
77BC0000	00058000	77BCF2A1	msvcrt	7.	
77CF0000	0008F000	UserClie	USER32	5.	
77D80000	00091000	77D86284	RPCRT4	5.	
77E20000	00046000	77E263CA	GDI32	5.	
77E70000	00076000	77E751D3	SHLWAPI	6.	
77F50000	0009B000	77F570D4	ADVAPI32	5.	

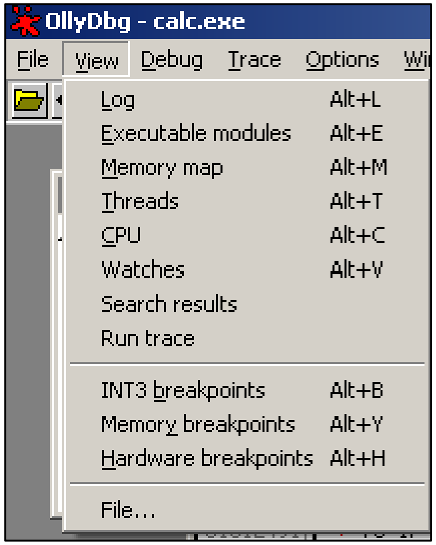
OllyDbg

- **Memory Map View -‘Alt + M’**



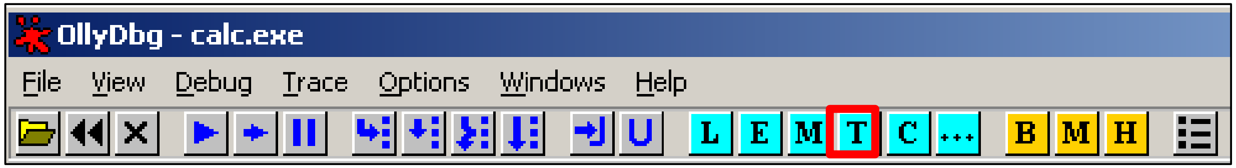


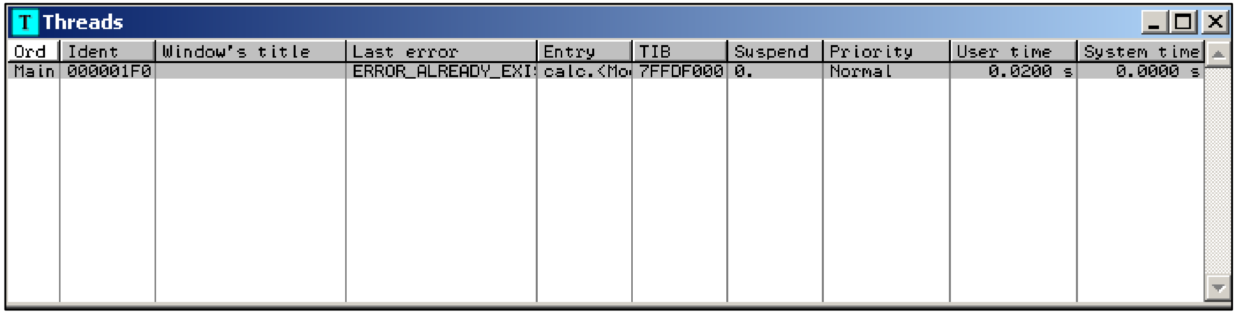
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00001000			Environment	Priv	RW	RW	
00020000	00001000			Process Parameter	Priv	RW	RW	
00030000	00005000				Priv	RW	RW	
0007C000	00001000				Priv	RW Gua	RW Gua	
0007D000	00003000			Stack of main thr	Priv	RW	RW	
00080000	00003000				Map	R	R	
00090000	00002000				Map	R	R	
000A0000	00009000				Priv	RW	RW	
001A0000	00006000				Priv	RW	RW	
001B0000	00003000				Map	RW	RW	
001C0000	00016000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
001E0000	0003D000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
00220000	00041000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
00270000	00006000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
00280000	00041000				Map	R	R	
002D0000	00002000				Map	R E	R E	
00390000	00002000				Map	R E	R E	
003A0000	00008000				Priv	RW	RW	
003B0000	00001000				Priv	RW	RW	
003C0000	00001000				Priv	RW	RW	
003D0000	00002000				Map	R	R	
003F0000	00002000				Map	R	R	
00400000	00008000				Priv	RW	RW	
00410000	00004000				Priv	RW	RW	
00420000	00003000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\
00430000	00003000				Priv	RW	RW	
00470000	00103000			GDI handles	Map	R	R	
00580000	00030000				Map	R E	R E	
00880000	00001000				Priv	RW	RW	
01000000	00001000	calc		PE header	Img	R	RWE Cop	
01001000	00013000	calc	.text	Code, imports	Img	R E	RWE Cop	



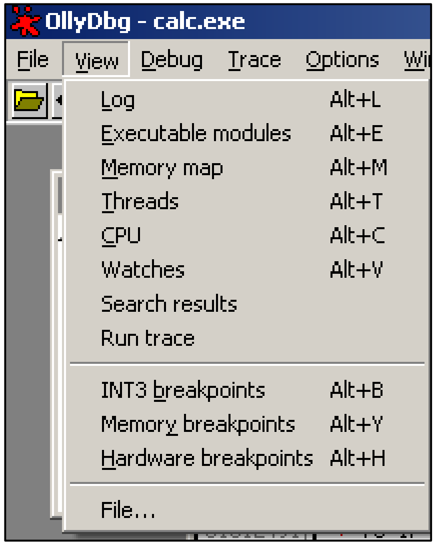
OllyDbg

- **Threads View -‘Alt + T’**



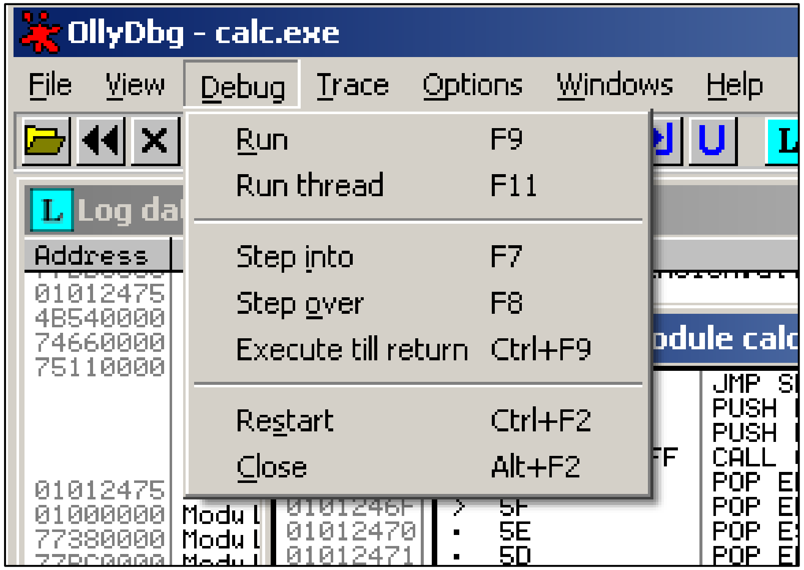

Threads

Ord	Ident	Window's title	Last error	Entry	TIB	Suspend	Priority	User time	System time
Main	000001F0		ERROR_ALREADY_EXI:	calc.<Mo	7FFDF000	0.	Normal	0.0200 s	0.0000 s



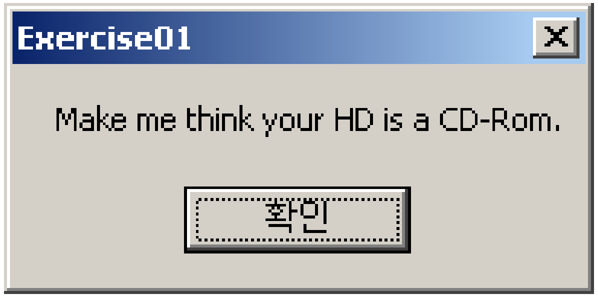
OllyDbg

- **Debug Menu**
  - Run -‘F9’
  - Pause -‘F12’
  - Step into -‘F7’
  - Step over -‘F8’
  - Execute till return -‘Ctrl + F9’
  - Execute till user code -‘Alt + F9’
  - Restart -‘Ctrl + F2’
  - Close -‘Alt + F2’



OllyDbg

- **Back To User Mode (1/4)**
  - Pause (‘F12’) + Execute till user code (‘Alt + F9’)

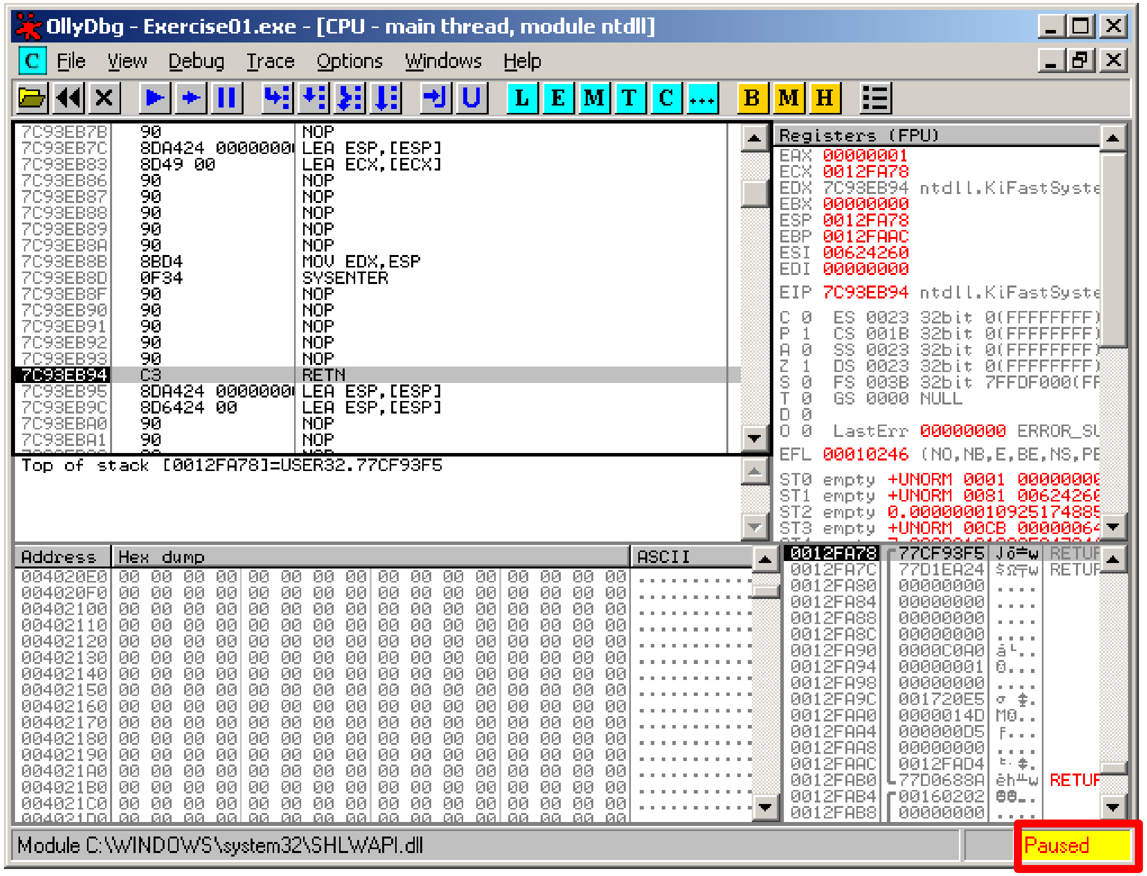


Make me think your HD is a CD-Rom.

  - MessageBox(), scanf() 등의 멈춰 있는 상태에서 활용
  - ex) MessageBox()호출 위치 찾기

OllyDbg

- **Back To User Mode (2/4)**
  - Pause -‘F12’



OllyDbg - Exercise01.exe - [CPU - main thread, module ntdll]

```
7C93EB7B   90               NOP
7C93EB7C   8DA424 0000000   LEA ESP,[ESP]
7C93EB83   8D49 00          LEA ECX,[ECX]
7C93EB86   90               NOP
7C93EB87   90               NOP
7C93EB88   90               NOP
7C93EB89   90               NOP
7C93EB8A   90               NOP
7C93EB8B   8BD4             MOV EDX,ESP
7C93EB8D   0F34             SYSENTER
7C93EB8F   90               NOP
7C93EB90   90               NOP
7C93EB91   90               NOP
7C93EB92   90               NOP
7C93EB93   90               NOP
7C93EB94   C3               RETN
7C93EB95   8DA424 0000000   LEA ESP,[ESP]
7C93EB9C   8D6424 00        LEA ESP,[ESP]
7C93EBA0   90               NOP
7C93EBA1   90               NOP
Top of stack [0012FA78]=USER32.77CF93F5
```

```
Registers (FPU)
EAX 00000001
ECX 0012FA78
EDX 7C93EB94 ntdll.KiFastSyste
EBX 00000000
ESP 0012FA78
EBP 0012FAAC
ESI 00624260
EDI 00000000

EIP 7C93EB94 ntdll.KiFastSyste

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FF
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SU

EFL 00010246 (NO,NB,E,BE,NS,PE

ST0 empty +UNORM 0001 0000000
ST1 empty +UNORM 0081 0062426
ST2 empty 0.000000010925174885
ST3 empty +UNORM 00CB 0000006
```

```
Address   Hex dump                                          ASCII
004020E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
004020F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
00402190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
004021A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
004021B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
004021C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...........
```

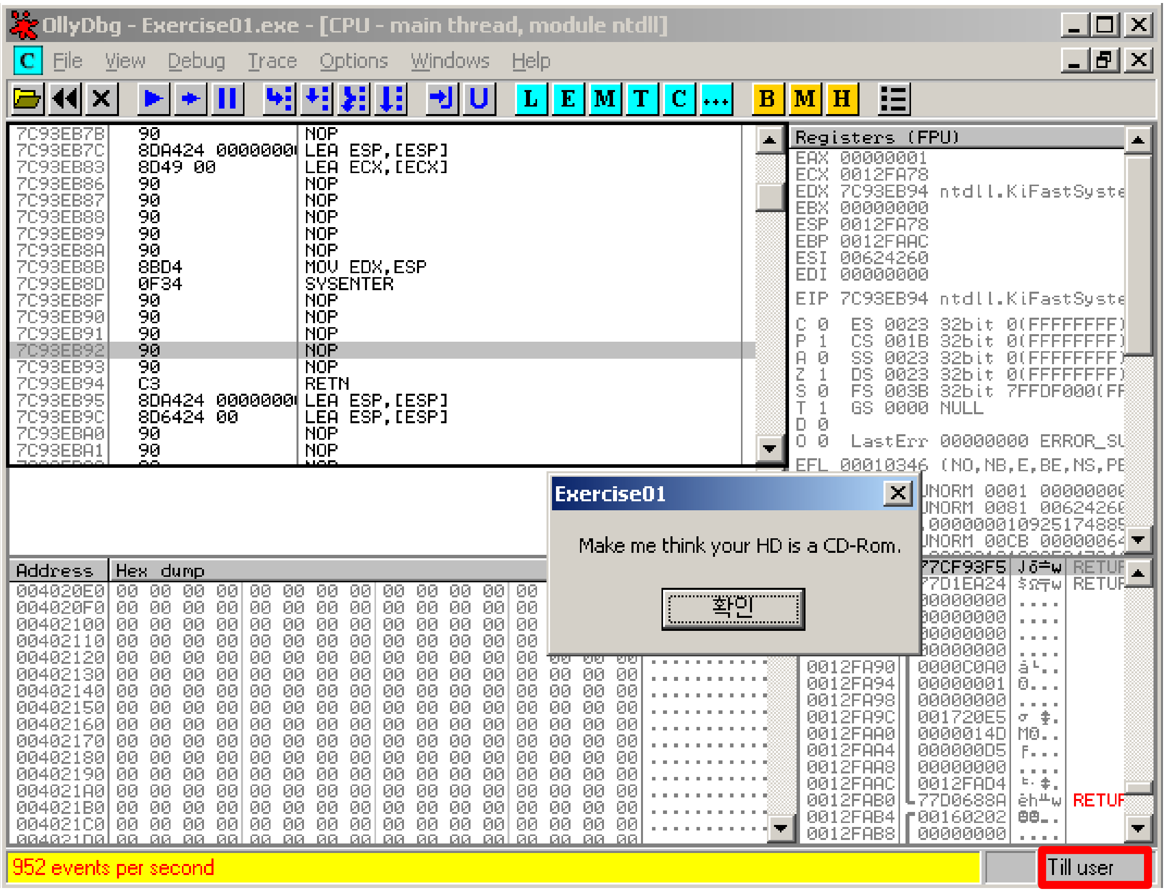
```
0012FA78  77CF93F5  Jõ≐w  RETUF
0012FA7C  77D1EA24  $Ω╤w  RETUF
0012FA80  00000000  ....
0012FA84  00000000  ....
0012FA88  00000000  ....
0012FA8C  00000000  ....
0012FA90  0000C0A0  á└..
0012FA94  00000001  ☺...
0012FA98  00000000  ....
0012FA9C  001720E5  σ ‡.
0012FAA0  0000014D  M☺..
0012FAA4  000000D5  F...
0012FAA8  00000000  ....
0012FAAC  0012FAD4  ╘·‡.
0012FAB0  77D0688A  èh╨w  RETUF
0012FAB4  00160202  ☻☻▬.
0012FAB8  00000000  ....
```

Module C:\WINDOWS\system32\SHLWAPI.dll

Paused

OllyDbg

- **Back To User Mode (3/4)**
  - Execute till user code (‘Alt + F9’)



OllyDbg - Exercise01.exe - [CPU - main thread, module ntdll]

```
7C93EB7B    90              NOP
7C93EB7C    8DA424 0000000  LEA ESP,[ESP]
7C93EB83    8D49 00         LEA ECX,[ECX]
7C93EB86    90              NOP
7C93EB87    90              NOP
7C93EB88    90              NOP
7C93EB89    90              NOP
7C93EB8A    90              NOP
7C93EB8B    8BD4            MOV EDX,ESP
7C93EB8D    0F34            SYSENTER
7C93EB8F    90              NOP
7C93EB90    90              NOP
7C93EB91    90              NOP
7C93EB92    90              NOP
7C93EB93    90              NOP
7C93EB94    C3              RETN
7C93EB95    8DA424 0000000  LEA ESP,[ESP]
7C93EB9C    8D6424 00       LEA ESP,[ESP]
7C93EBA0    90              NOP
7C93EBA1    90              NOP
```

```
Registers (FPU)
EAX 00000001
ECX 0012FA78
EDX 7C93EB94 ntdll.KiFastSyste
EBX 00000000
ESP 0012FA78
EBP 0012FAAC
ESI 00624260
EDI 00000000

EIP 7C93EB94 ntdll.KiFastSyste

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FF
T 1  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SU

EFL 00010346 (NO,NB,E,BE,NS,PE
UNORM 0001 0000000
UNORM 0081 0062426
.00000001092517488
UNORM 00CB 0000006
```

Exercise01

Make me think your HD is a CD-Rom.

확인

```
Address   Hex dump
004020E0  00 00 00 00 00 00 00 00 00 00 00 00 00
004020F0  00 00 00 00 00 00 00 00 00 00 00 00 00
00402100  00 00 00 00 00 00 00 00 00 00 00 00 00
00402110  00 00 00 00 00 00 00 00 00 00 00 00 00
00402120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00402130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

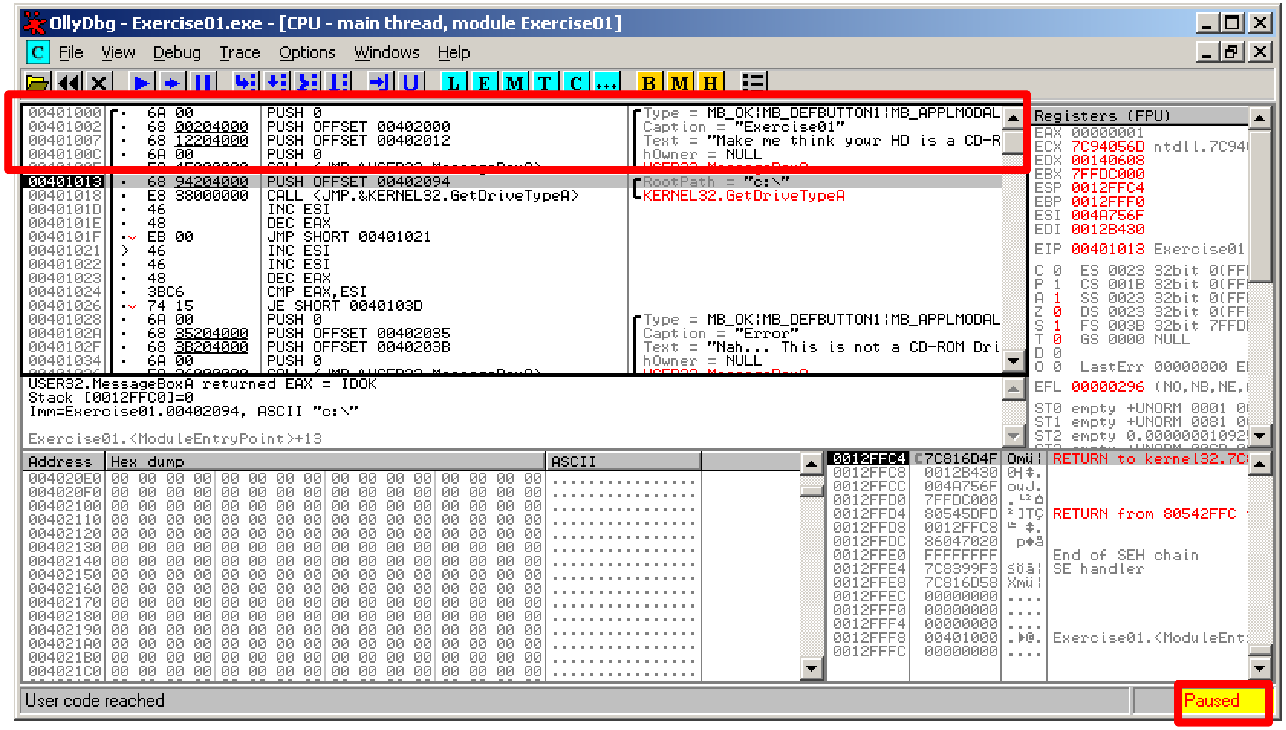
```
          77CF93F5  J õ=w  RETUF
          77D1EA24  $ΩΤw   RETUF
          00000000  ....
          00000000  ....
          00000000  ....
          00000000  ....
0012FA90  0000C0A0  à└..
0012FA94  00000001  ☺...
0012FA98  00000000  ....
0012FA9C  001720E5  σ ‡.
0012FAA0  0000014D  M☺..
0012FAA4  000000D5  ╒...
0012FAA8  00000000  ....
0012FAAC  0012FAD4  ╘·‡.
0012FAB0  77D0688A  èh╨w   RETUF
0012FAB4  00160202  ☻☻▬.
0012FAB8  00000000  ....
```

952 events per second

Till user

OllyDbg

- **Back To User Mode (4/4)**
  - Click MessageBox



OllyDbg - Exercise01.exe - [CPU - main thread, module Exercise01]
C File View Debug Trace Options Windows Help
L E M T C ... B M H

```
00401000  ┌.  6A 00          PUSH 0                                ┌Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
00401002  │.  68 00204000    PUSH OFFSET 00402000                  │Caption = "Exercise01"
00401007  │.  68 12204000    PUSH OFFSET 00402012                  │Text = "Make me think your HD is a CD-R
0040100C  │.  6A 00          PUSH 0                                │hOwner = NULL
00401013  │.  68 94204000    PUSH OFFSET 00402094                  ┌RootPath = "c:\"
00401018  │.  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>    └KERNEL32.GetDriveTypeA
0040101D  │.  46             INC ESI
0040101E  │.  48             DEC EAX
0040101F  │.v EB 00          JMP SHORT 00401021
00401021  │>  46             INC ESI
00401022  │.  46             INC ESI
00401023  │.  48             DEC EAX
00401024  │.  3BC6           CMP EAX,ESI
00401026  │.v 74 15          JE SHORT 0040103D
00401028  │.  6A 00          PUSH 0                                ┌Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
0040102A  │.  68 35204000    PUSH OFFSET 00402035                  │Caption = "Error"
0040102F  │.  68 3B204000    PUSH OFFSET 0040203B                  │Text = "Nah... This is not a CD-ROM Dri
00401034  │.  6A 00          PUSH 0                                │hOwner = NULL
```

```
USER32.MessageBoxA returned EAX = IDOK
Stack [0012FFC0]=0
Imm=Exercise01.00402094, ASCII "c:\"

Exercise01.<ModuleEntryPoint>+13
```

```
Registers (FPU)
EAX 00000001
ECX 7C94056D ntdll.7C94
EDX 00140608
EBX 7FFDC000
ESP 0012FFC4
EBP 0012FFF0
ESI 004A756F
EDI 0012B430

EIP 00401013 Exercise01

C 0  ES 0023 32bit 0(FF
P 1  CS 001B 32bit 0(FF
A 1  SS 0023 32bit 0(FF
Z 0  DS 0023 32bit 0(FF
S 1  FS 003B 32bit 7FFD
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 E

EFL 00000296 (NO,NB,NE,

ST0 empty +UNORM 0001 0
ST1 empty +UNORM 0081 0
ST2 empty 0.00000001092
```

```
Address   Hex dump                                          ASCII
004020E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004020F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00402190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004021C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

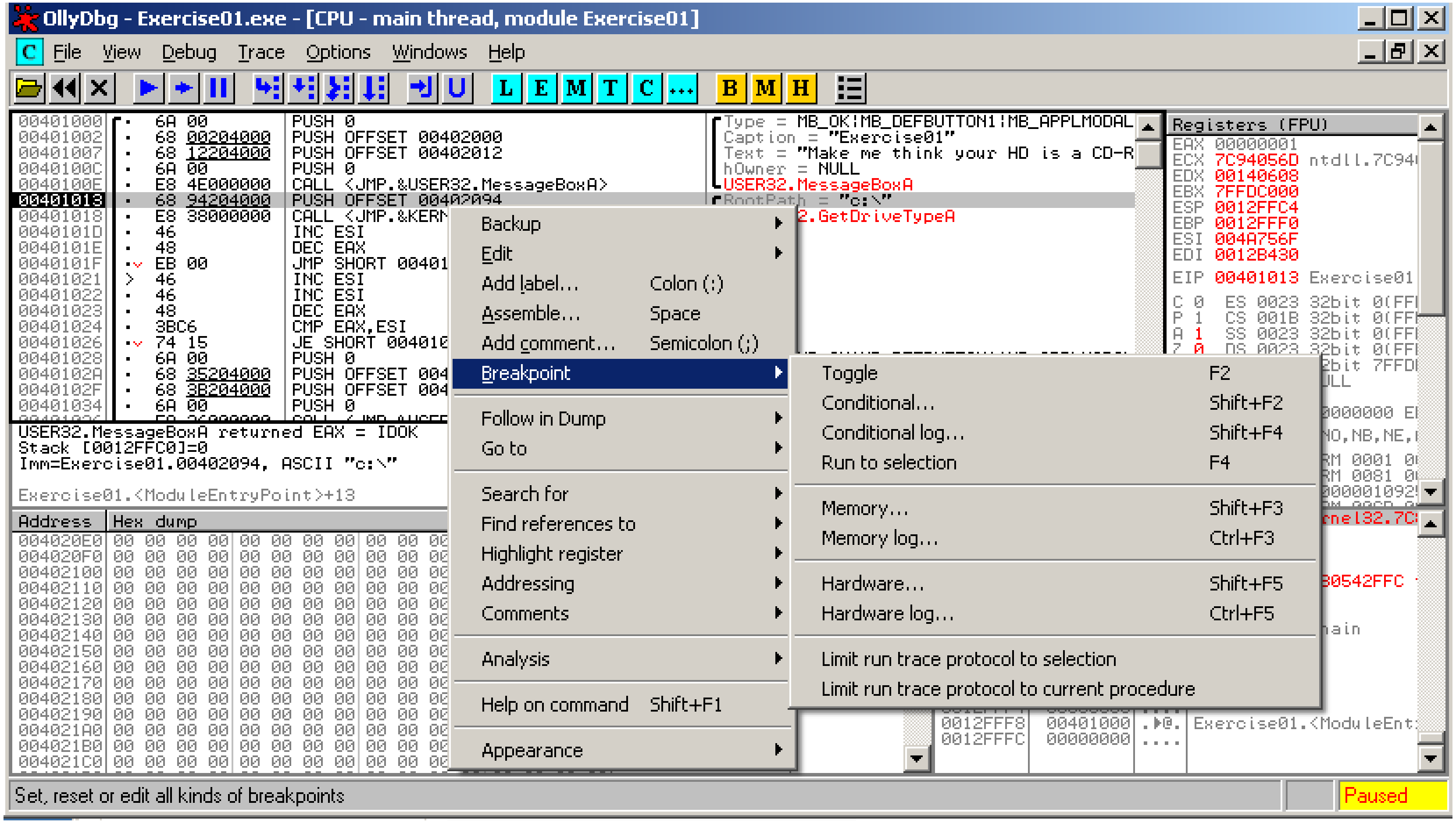
```
0012FFC4  7C816D4F  Omü¦  RETURN to kernel32.7C
0012FFC8  0012B430  0┤‡.
0012FFCC  004A756F  ouJ.
0012FFD0  7FFDC000  .└²⌂
0012FFD4  80545DFD  ²]TÇ  RETURN from 80542FFC
0012FFD8  0012FFC8  ╚ ‡.
0012FFDC  86047020   p♦å
0012FFE0  FFFFFFFF        End of SEH chain
0012FFE4  7C8399F3  ≤Öâ¦  SE handler
0012FFE8  7C816D58  Xmü¦
0012FFEC  00000000  ....
0012FFF0  00000000  ....
0012FFF4  00000000  ....
0012FFF8  00401000  .►@.  Exercise01.<ModuleEnt
0012FFFC  00000000  ....
```

User code reached

Paused

OllyDbg

- **Breakpoint**



```
00401000  ┌.  6A 00         PUSH 0
00401002  │.  68 00204000   PUSH OFFSET 00402000
00401007  │.  68 12204000   PUSH OFFSET 00402012
0040100C  │.  6A 00         PUSH 0
0040100E  │.  E8 4E000000   CALL <JMP.&USER32.MessageBoxA>
00401013  │.  68 94204000   PUSH OFFSET 00402094
00401018  │.  E8 38000000   CALL <JMP.&KERN
0040101D  │.  46            INC ESI
0040101E  │.  48            DEC EAX
0040101F  │.v EB 00         JMP SHORT 00401
00401021  │>  46            INC ESI
00401022  │.  46            INC ESI
00401023  │.  48            DEC EAX
00401024  │.  3BC6          CMP EAX,ESI
00401026  │.v 74 15         JE SHORT 004010
00401028  │.  6A 00         PUSH 0
0040102A  │.  68 35204000   PUSH OFFSET 004
0040102F  │.  68 3B204000   PUSH OFFSET 004
00401034  │.  6A 00         PUSH 0
```

```
┌Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
│Caption = "Exercise01"
│Text = "Make me think your HD is a CD-R
│hOwner = NULL
└USER32.MessageBoxA
┌RootPath = "c:\"
2.GetDriveTypeA
```

```
USER32.MessageBoxA returned EAX = IDOK
Stack [0012FFC0]=0
Imm=Exercise01.00402094, ASCII "c:\"

Exercise01.<ModuleEntryPoint>+13
```

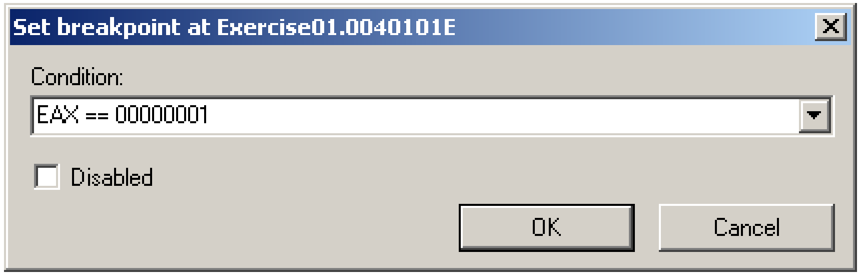
```
Registers (FPU)
EAX 00000001
ECX 7C94056D ntdll.7C94
EDX 00140608
EBX 7FFDC000
ESP 0012FFC4
EBP 0012FFF0
ESI 004A756F
EDI 0012B430

EIP 00401013 Exercise01

C 0  ES 0023 32bit 0(FF
P 1  CS 001B 32bit 0(FF
A 1  SS 0023 32bit 0(FF
Z 0  DS 0023 32bit 0(FF
```

```
Address   Hex dump
004020E0  00 00 00 00 00 00 00 00 00 00 00
004020F0  00 00 00 00 00 00 00 00 00 00 00
00402100  00 00 00 00 00 00 00 00 00 00 00
00402110  00 00 00 00 00 00 00 00 00 00 00
00402120  00 00 00 00 00 00 00 00 00 00 00
00402130  00 00 00 00 00 00 00 00 00 00 00
00402140  00 00 00 00 00 00 00 00 00 00 00
00402150  00 00 00 00 00 00 00 00 00 00 00
00402160  00 00 00 00 00 00 00 00 00 00 00
00402170  00 00 00 00 00 00 00 00 00 00 00
00402180  00 00 00 00 00 00 00 00 00 00 00
00402190  00 00 00 00 00 00 00 00 00 00 00
004021A0  00 00 00 00 00 00 00 00 00 00 00
004021B0  00 00 00 00 00 00 00 00 00 00 00
004021C0  00 00 00 00 00 00 00 00 00 00 00
```

```
0012FFF8  00401000  .▶@.  Exercise01.<ModuleEnt
0012FFFC  00000000  ....
```

OllyDbg

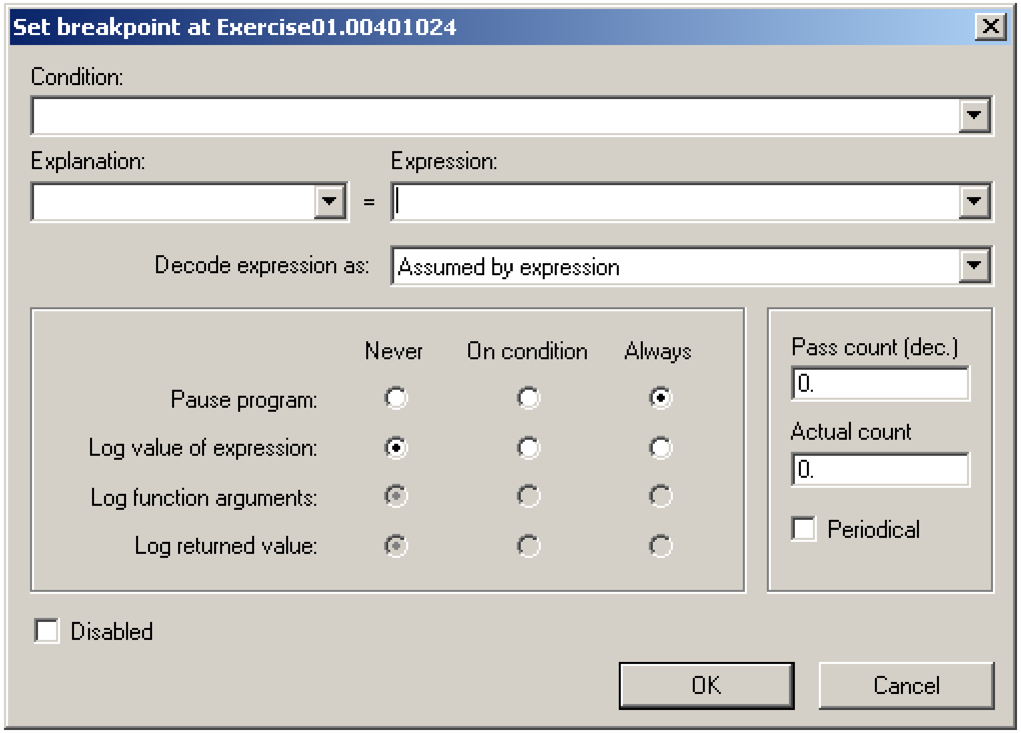
- **Software Breakpoint**
  - Toggle -‘F2’
  - Conditional -‘Shift + F2’
  - Conditional Log -‘Shift + F4’
  - Run to Selection -‘F4’



Set breakpoint at Exercise01.0040101E

Condition: EAX == 00000001

☐ Disabled



Set breakpoint at Exercise01.00401024

Condition:

Explanation: = Expression:

Decode expression as: Assumed by expression

	Never	On condition	Always
Pause program:	○	○	●
Log value of expression:	●	○	○
Log function arguments:	●	○	○
Log returned value:	●	○	○

Pass count (dec.) 0.

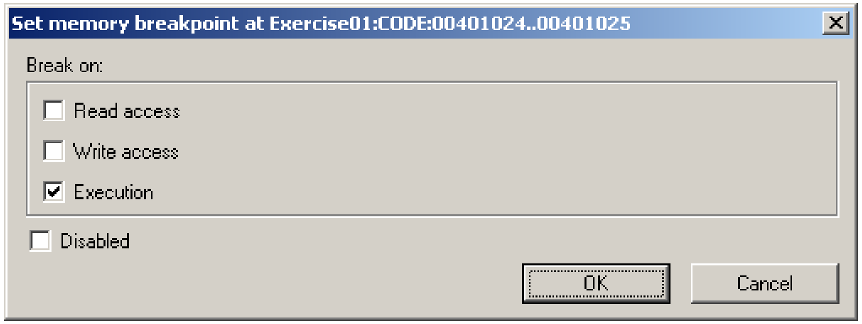
Actual count 0.

☐ Periodical

☐ Disabled

OllyDbg

- **Memory Breakpoint**
  - Memory -‘Shift + F3’
  - Memory Log -‘Ctrl + F3’
  - Only 1 Memory Breakpoint

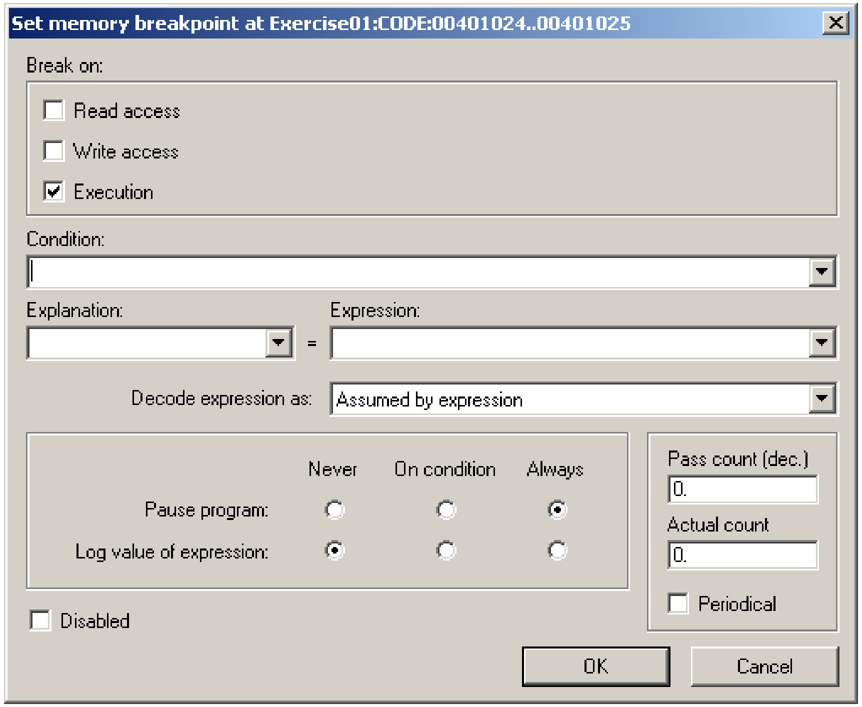


Set memory breakpoint at Exercise01:CODE:00401024..00401025

Break on:

- ☐ Read access
- ☐ Write access
- ☑ Execution

☐ Disabled



Set memory breakpoint at Exercise01:CODE:00401024..00401025

Break on:

- ☐ Read access
- ☐ Write access
- ☑ Execution

Condition:

Explanation: = Expression:

Decode expression as: Assumed by expression

	Never	On condition	Always
Pause program:	○	○	●
Log value of expression:	●	○	○

Pass count (dec.) 0.

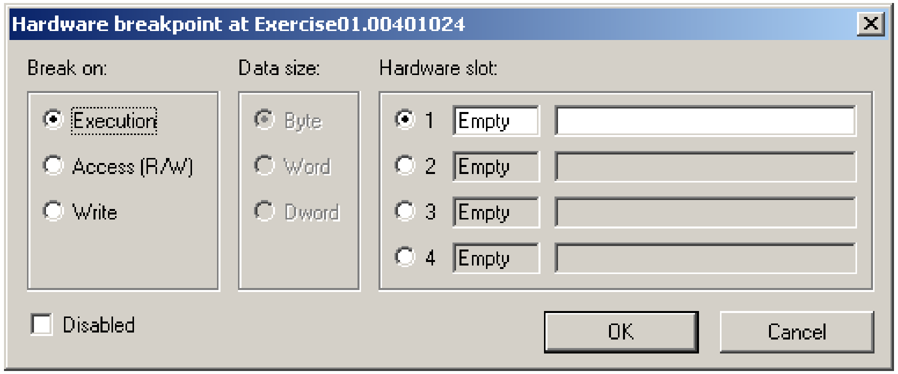
Actual count 0.

☐ Periodical

☐ Disabled

OllyDbg

- **Hardware Breakpoint**
  - Hardware -‘Shift + F5’
  - Hardware Log -‘Ctrl + F5’
  - Only 4 Hardware Breakpoints



Hardware breakpoint at Exercise01.00401024

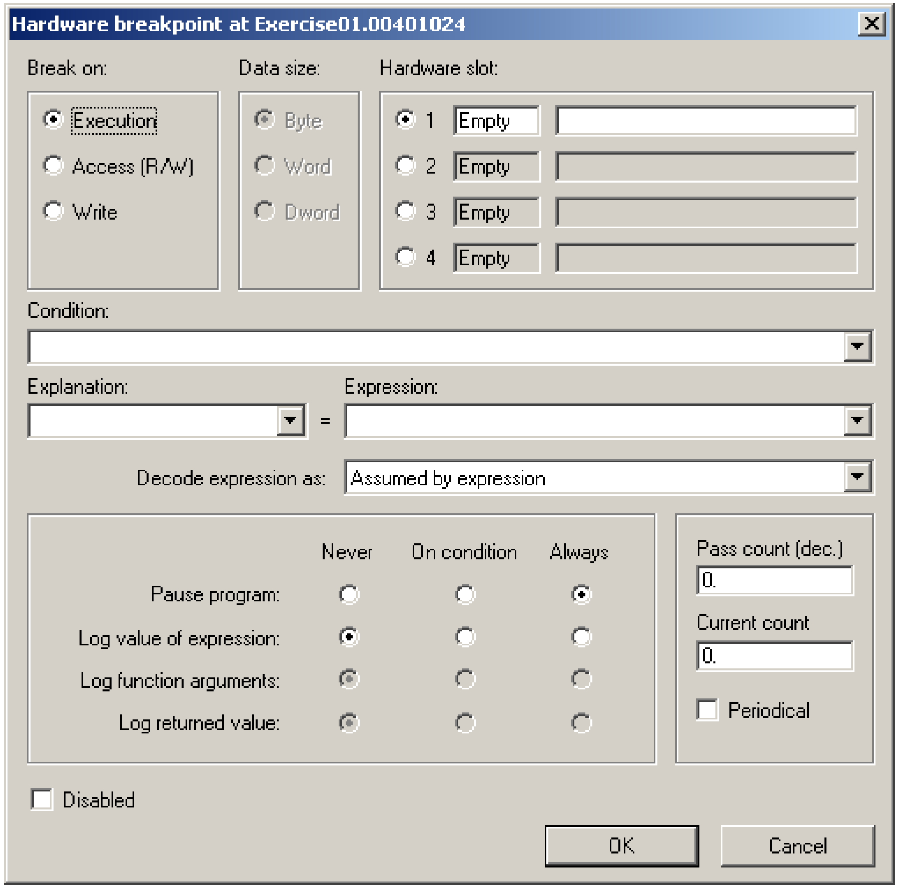
Break on: ● Execution ○ Access (R/W) ○ Write

Data size: ● Byte ○ Word ○ Dword

Hardware slot:

● 1	Empty	
○ 2	Empty	
○ 3	Empty	
○ 4	Empty	

☐ Disabled



Hardware breakpoint at Exercise01.00401024

Break on: ● Execution ○ Access (R/W) ○ Write

Data size: ● Byte ○ Word ○ Dword

Hardware slot:

● 1	Empty	
○ 2	Empty	
○ 3	Empty	
○ 4	Empty	

Condition:

Explanation: =

Expression:

Decode expression as: Assumed by expression

	Never	On condition	Always
Pause program:	○	○	●
Log value of expression:	●	○	○
Log function arguments:	●	○	○
Log returned value:	●	○	○

Pass count (dec.) 0.

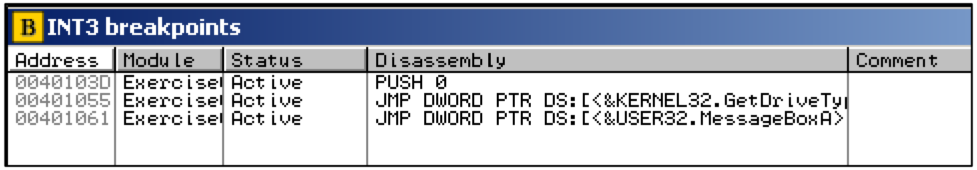
Current count 0.

☐ Periodical

☐ Disabled

OllyDbg

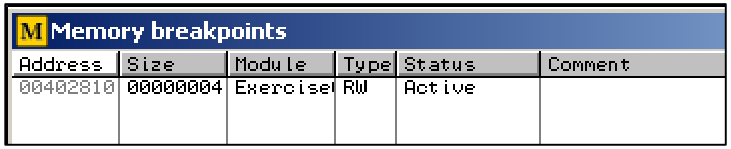
- **Breakpoint Views**
  - Software (INT 3) Breakpoints -‘Alt + B’



B INT3 breakpoints

Address	Module	Status	Disassembly	Comment
0040103D	Exercise	Active	PUSH 0	
00401055	Exercise	Active	JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy	
00401061	Exercise	Active	JMP DWORD PTR DS:[<&USER32.MessageBoxA>	

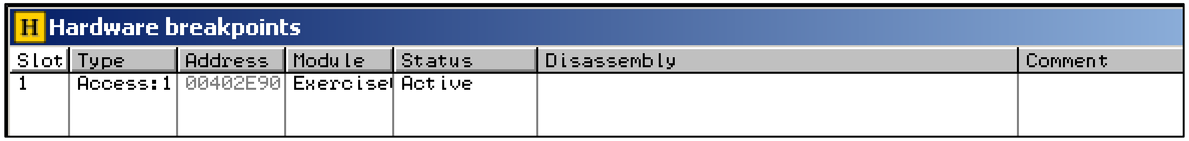
  - Memory Breakpoints -‘Alt + Y’



M Memory breakpoints

Address	Size	Module	Type	Status	Comment
00402810	00000004	Exercise	RW	Active	

  - Hardware Breakpoints -‘Alt + H’

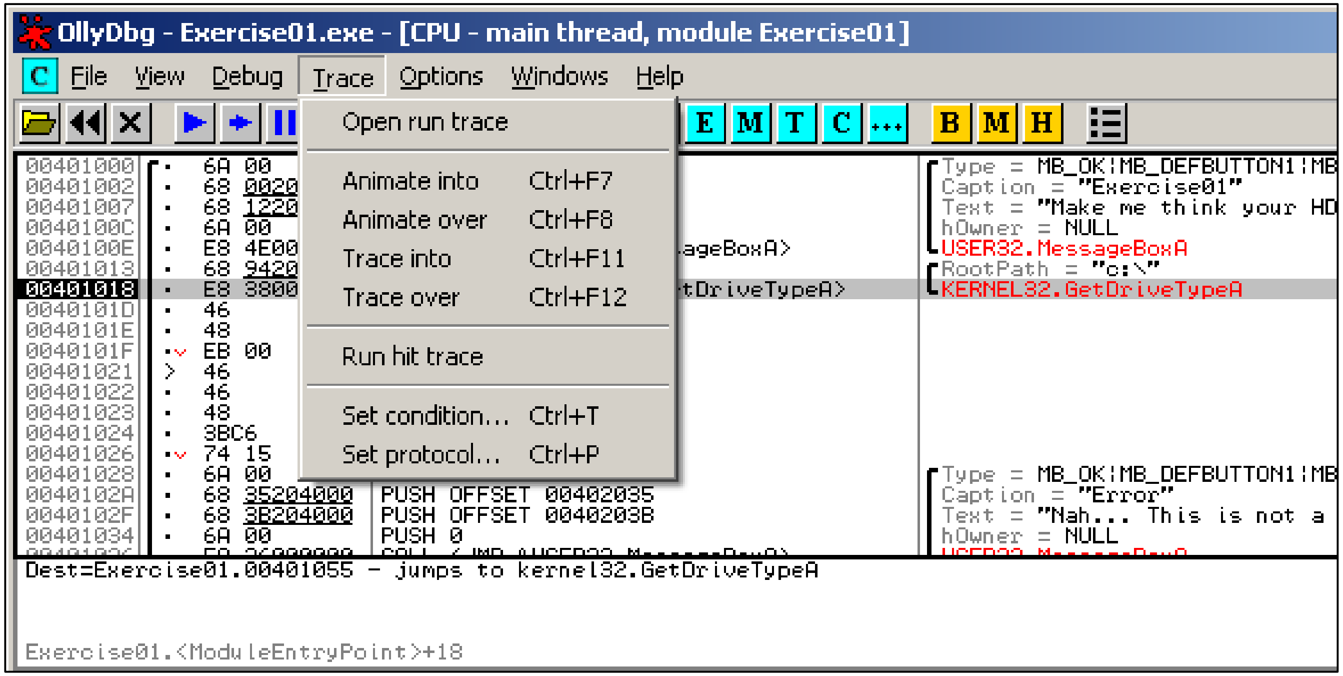


H Hardware breakpoints

Slot	Type	Address	Module	Status	Disassembly	Comment
1	Access:1	00402E90	Exercise	Active		

OllyDbg

- **Trace Menu**



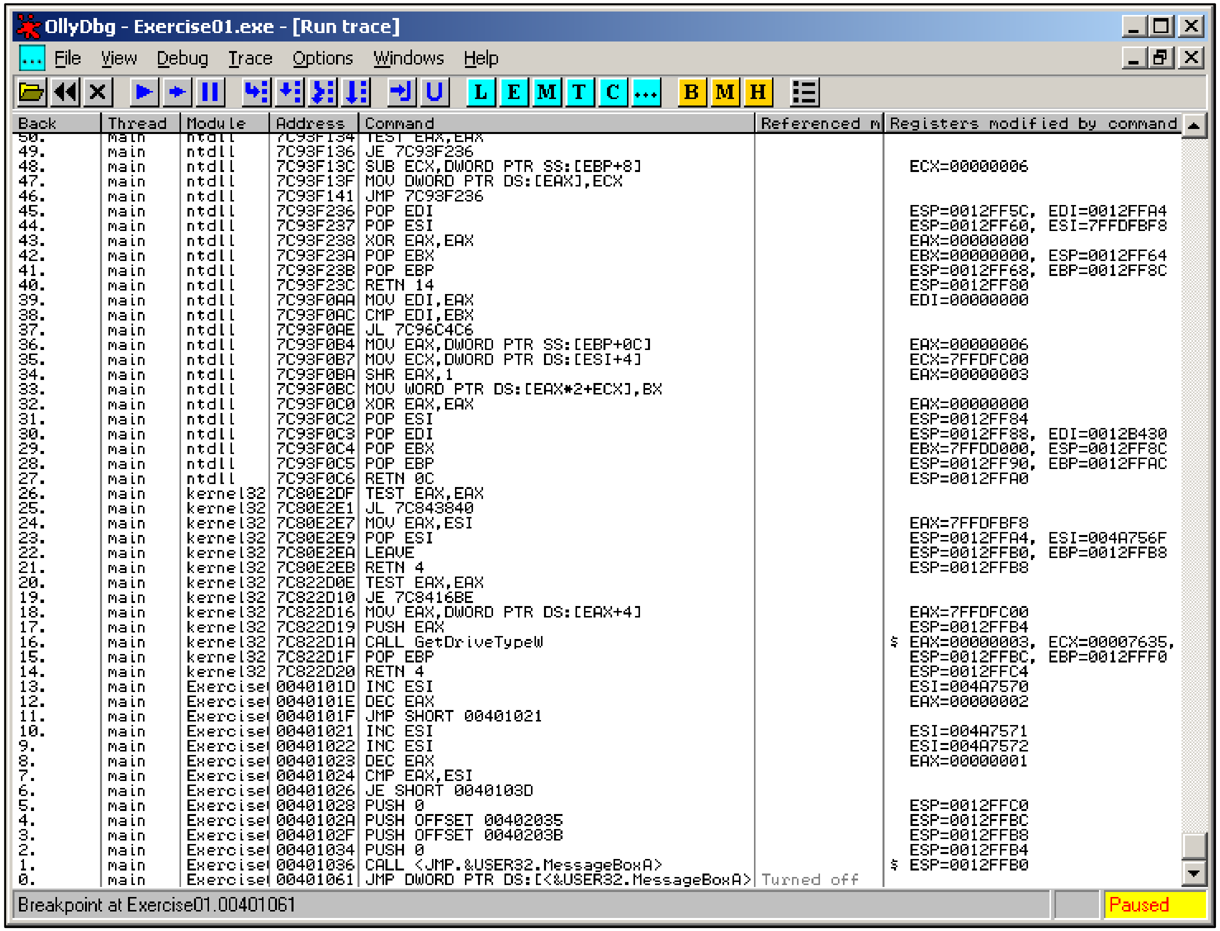
```
00401000 ┌.  6A 00
00401002 │.  68 0020
00401007 │.  68 1220
0040100C │.  6A 00
0040100E │.  E8 4E00                              ageBoxA>
00401013 │.  68 9420
00401018 │.  E8 3800                              tDriveTypeA>
0040101D │.  46
0040101E │.  48
0040101F │.v EB 00
00401021 │>  46
00401022 │.  46
00401023 │.  48
00401024 │.  3BC6
00401026 │.v 74 15
00401028 │.  6A 00
0040102A │.  68 35204000     PUSH OFFSET 00402035
0040102F │.  68 3B204000     PUSH OFFSET 0040203B
00401034 │.  6A 00           PUSH 0
```

```
┌Type = MB_OK|MB_DEFBUTTON1|MB
│Caption = "Exercise01"
│Text = "Make me think your HD
│hOwner = NULL
└USER32.MessageBoxA
┌RootPath = "c:\"
└KERNEL32.GetDriveTypeA

┌Type = MB_OK|MB_DEFBUTTON1|MB
│Caption = "Error"
│Text = "Nah... This is not a
│hOwner = NULL
```

```
Dest=Exercise01.00401055 - jumps to kernel32.GetDriveTypeA

Exercise01.<ModuleEntryPoint>+18
```

OllyDbg

- Animate into -‘Ctrl + F7’
- Animate over -‘Ctrl + F8’
- Trace into -‘Ctrl + F11’
- Trace over -‘Ctrl + F12’

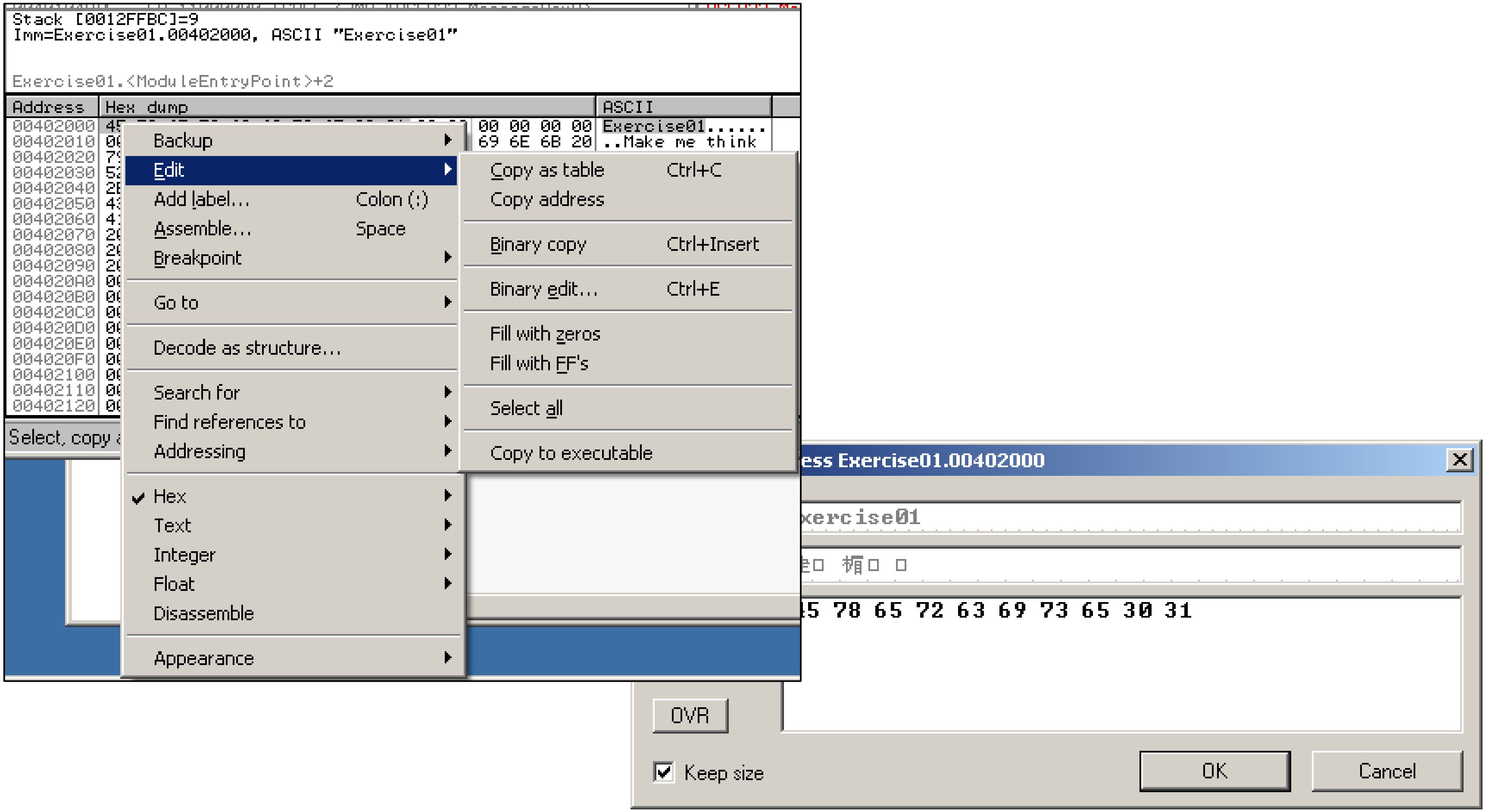


```
Back  Thread  Module    Address   Command                                     Referenced m  Registers modified by command
50.   main    ntdll     7C93F134  TEST EAX,EAX
49.   main    ntdll     7C93F136  JE 7C93F236
48.   main    ntdll     7C93F13C  SUB ECX,DWORD PTR SS:[EBP+8]                                 ECX=00000006
47.   main    ntdll     7C93F13F  MOV DWORD PTR DS:[EAX],ECX
46.   main    ntdll     7C93F141  JMP 7C93F236
45.   main    ntdll     7C93F236  POP EDI                                                      ESP=0012FF5C, EDI=0012FFA4
44.   main    ntdll     7C93F237  POP ESI                                                      ESP=0012FF60, ESI=7FFDFBF8
43.   main    ntdll     7C93F238  XOR EAX,EAX                                                  EAX=00000000
42.   main    ntdll     7C93F23A  POP EBX                                                      EBX=00000000, ESP=0012FF64
41.   main    ntdll     7C93F23B  POP EBP                                                      ESP=0012FF68, EBP=0012FF8C
40.   main    ntdll     7C93F23C  RETN 14                                                      ESP=0012FF80
39.   main    ntdll     7C93F0AA  MOV EDI,EAX                                                  EDI=00000000
38.   main    ntdll     7C93F0AC  CMP EDI,EBX
37.   main    ntdll     7C93F0AE  JL 7C96C4C6
36.   main    ntdll     7C93F0B4  MOV EAX,DWORD PTR SS:[EBP+0C]                                EAX=00000006
35.   main    ntdll     7C93F0B7  MOV ECX,DWORD PTR DS:[ESI+4]                                 ECX=7FFDFC00
34.   main    ntdll     7C93F0BA  SHR EAX,1                                                    EAX=00000003
33.   main    ntdll     7C93F0BC  MOV WORD PTR DS:[EAX*2+ECX],BX
32.   main    ntdll     7C93F0C0  XOR EAX,EAX                                                  EAX=00000000
31.   main    ntdll     7C93F0C2  POP ESI                                                      ESP=0012FF84
30.   main    ntdll     7C93F0C3  POP EDI                                                      ESP=0012FF88, EDI=0012B430
29.   main    ntdll     7C93F0C4  POP EBX                                                      EBX=7FFDD000, ESP=0012FF8C
28.   main    ntdll     7C93F0C5  POP EBP                                                      ESP=0012FF90, EBP=0012FFAC
27.   main    ntdll     7C93F0C6  RETN 0C                                                      ESP=0012FFA0
26.   main    kernel32  7C80E2DF  TEST EAX,EAX
25.   main    kernel32  7C80E2E1  JL 7C843840
24.   main    kernel32  7C80E2E7  MOV EAX,ESI                                                  EAX=7FFDFBF8
23.   main    kernel32  7C80E2E9  POP ESI                                                      ESP=0012FFA4, ESI=004A756F
22.   main    kernel32  7C80E2EA  LEAVE                                                        ESP=0012FFB0, EBP=0012FFB8
21.   main    kernel32  7C80E2EB  RETN 4                                                       ESP=0012FFB8
20.   main    kernel32  7C822D0E  TEST EAX,EAX
19.   main    kernel32  7C822D10  JE 7C8416BE
18.   main    kernel32  7C822D16  MOV EAX,DWORD PTR DS:[EAX+4]                                 EAX=7FFDFC00
17.   main    kernel32  7C822D19  PUSH EAX                                                     ESP=0012FFB4
16.   main    kernel32  7C822D1A  CALL GetDriveTypeW                                         $ EAX=00000003, ECX=00007635,
15.   main    kernel32  7C822D1F  POP EBP                                                      ESP=0012FFBC, EBP=0012FFF0
14.   main    kernel32  7C822D20  RETN 4                                                       ESP=0012FFC4
13.   main    Exercise  0040101D  INC ESI                                                      ESI=004A7570
12.   main    Exercise  0040101E  DEC EAX                                                      EAX=00000002
11.   main    Exercise  0040101F  JMP SHORT 00401021
10.   main    Exercise  00401021  INC ESI                                                      ESI=004A7571
9.    main    Exercise  00401022  INC ESI                                                      ESI=004A7572
8.    main    Exercise  00401023  DEC EAX                                                      EAX=00000001
7.    main    Exercise  00401024  CMP EAX,ESI
6.    main    Exercise  00401026  JE SHORT 0040103D
5.    main    Exercise  00401028  PUSH 0                                                       ESP=0012FFC0
4.    main    Exercise  0040102A  PUSH OFFSET 00402035                                         ESP=0012FFBC
3.    main    Exercise  0040102F  PUSH OFFSET 0040203B                                         ESP=0012FFB8
2.    main    Exercise  00401034  PUSH 0                                                       ESP=0012FFB4
1.    main    Exercise  00401036  CALL <JMP.&USER32.MessageBoxA>                             $ ESP=0012FFB0
0.    main    Exercise  00401061  JMP DWORD PTR DS:[<&USER32.MessageBoxA>  Turned off
```

Breakpoint at Exercise01.00401061

OllyDbg

- **Binary Edit -‘Ctrl + E’**



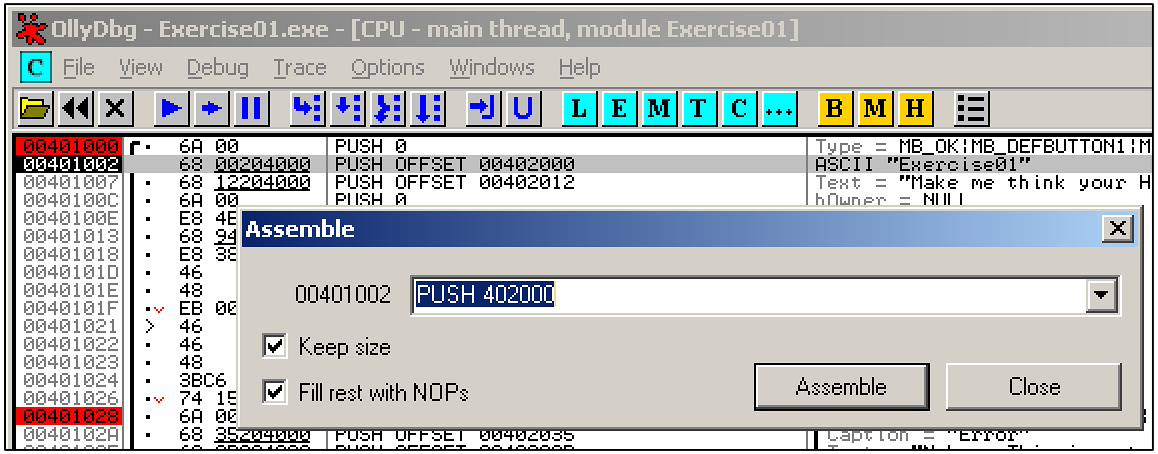
```
Stack [0012FFBC]=9
Imm=Exercise01.00402000, ASCII "Exercise01"

Exercise01.<ModuleEntryPoint>+2
```

```
Address   Hex dump                          ASCII
00402000  45 ...          00 00 00 00       Exercise01......
00402010  00 ...          69 6E 6B 20       ..Make me think
00402020  7
00402030  5
00402040  2
00402050  4
00402060  4
00402070  2
00402080  2
00402090  2
004020A0  0
004020B0  0
004020C0  0
004020D0  0
004020E0  0
004020F0  0
00402100  0
00402110  0
00402120  0
```

```
ess Exercise01.00402000
xercise01
5 78 65 72 63 69 73 65 30 31
```

OllyDbg

- **Assemble – ‘Space’**

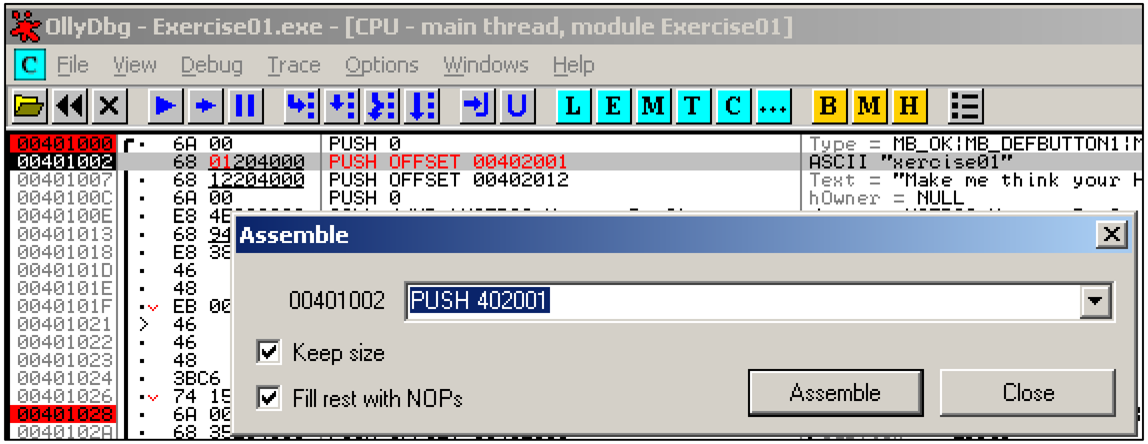

OllyDbg - Exercise01.exe - [CPU - main thread, module Exercise01]
C File View Debug Trace Options Windows Help
L E M T C ... B M H
Assemble
Assemble
Close

```
00401000  ┌.  6A 00          PUSH 0                       Type = MB_OK|MB_DEFBUTTON1|M
00401002  │   68 00204000    PUSH OFFSET 00402000         ASCII "Exercise01"
00401007  │.  68 12204000    PUSH OFFSET 00402012         Text = "Make me think your H
0040100C  │.  6A 00          PUSH 0                       hOwner = NULL
0040100E  │.  E8 4E
00401013  │.  68 94
00401018  │.  E8 38
0040101D  │.  46
0040101E  │.  48
0040101F  │.v  EB 00
00401021  │>  46
00401022  │.  46
00401023  │.  48
00401024  │.  3BC6
00401026  │.v  74 15
00401028  │.  6A 00
0040102A  │.  68 35204000    PUSH OFFSET 00402035         Caption = "Error"
```

00401002 PUSH 402000

☑ Keep size

☑ Fill rest with NOPs


OllyDbg - Exercise01.exe - [CPU - main thread, module Exercise01]
C File View Debug Trace Options Windows Help
L E M T C ... B M H
Assemble
Assemble
Close

```
00401000  ┌.  6A 00          PUSH 0                       Type = MB_OK|MB_DEFBUTTON1|M
00401002  │   68 01204000    PUSH OFFSET 00402001         ASCII "xercise01"
00401007  │.  68 12204000    PUSH OFFSET 00402012         Text = "Make me think your H
0040100C  │.  6A 00          PUSH 0                       hOwner = NULL
0040100E  │.  E8 4E
00401013  │.  68 94
00401018  │.  E8 38
0040101D  │.  46
0040101E  │.  48
0040101F  │.v  EB 00
00401021  │>  46
00401022  │.  46
00401023  │.  48
00401024  │.  3BC6
00401026  │.v  74 15
00401028  │.  6A 00
0040102A  │.  68 35
```

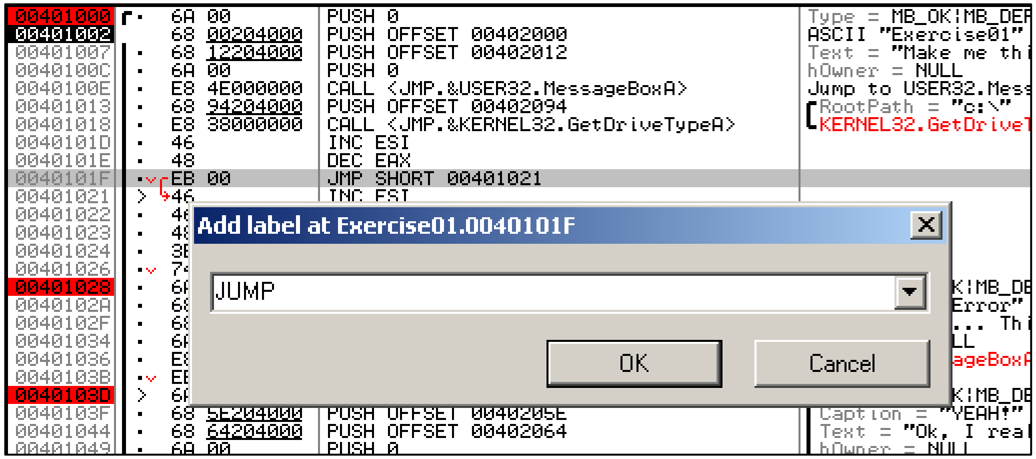
00401002 PUSH 402001

☑ Keep size

☑ Fill rest with NOPs

OllyDbg

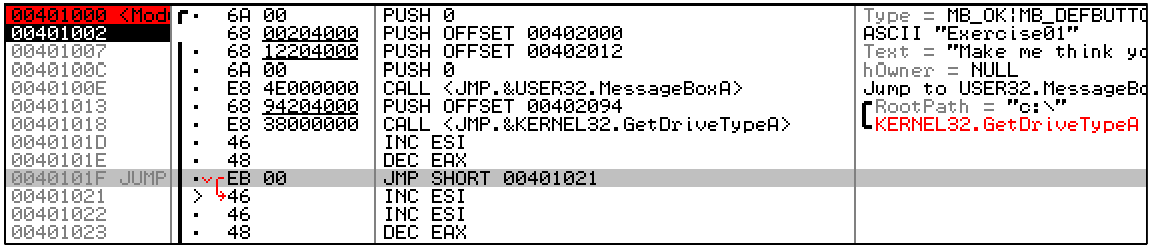
- **Add Label – ‘:’**



```
00401000 ┌.  6A 00          PUSH 0                                Type = MB_OK|MB_DEF
00401002  .  68 00204000    PUSH OFFSET 00402000                  ASCII "Exercise01"
00401007 |.  68 12204000    PUSH OFFSET 00402012                  Text = "Make me thi
0040100C |.  6A 00          PUSH 0                                hOwner = NULL
0040100E |.  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>        Jump to USER32.Mess
00401013 |.  68 94204000    PUSH OFFSET 00402094                 ┌RootPath = "c:\"
00401018 |.  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>   └KERNEL32.GetDriveT
0040101D |.  46             INC ESI
0040101E |.  48             DEC EAX
0040101F |.v┌EB 00          JMP SHORT 00401021
00401021 |> └46             INC ESI
00401022 |.  46
00401023 |.  48
00401024 |.  3E
00401026 |.v 74
00401028 |.  6A                                                   K|MB_DE
0040102A |.  68                                                   Error"
0040102F |.  68                                                   ... Thi
00401034 |.  6A                                                   LL
00401036 |.  E8                                                   ageBoxA
0040103B |.v EB
0040103D |>  6A                                                   K|MB_DE
0040103F |.  68 5E204000    PUSH OFFSET 0040205E                  Caption = "YEAH!"
00401044 |.  68 64204000    PUSH OFFSET 00402064                  Text = "Ok, I real
00401049 |.  6A 00          PUSH 0                                hOwner = NULL
```

Add label at Exercise01.0040101F

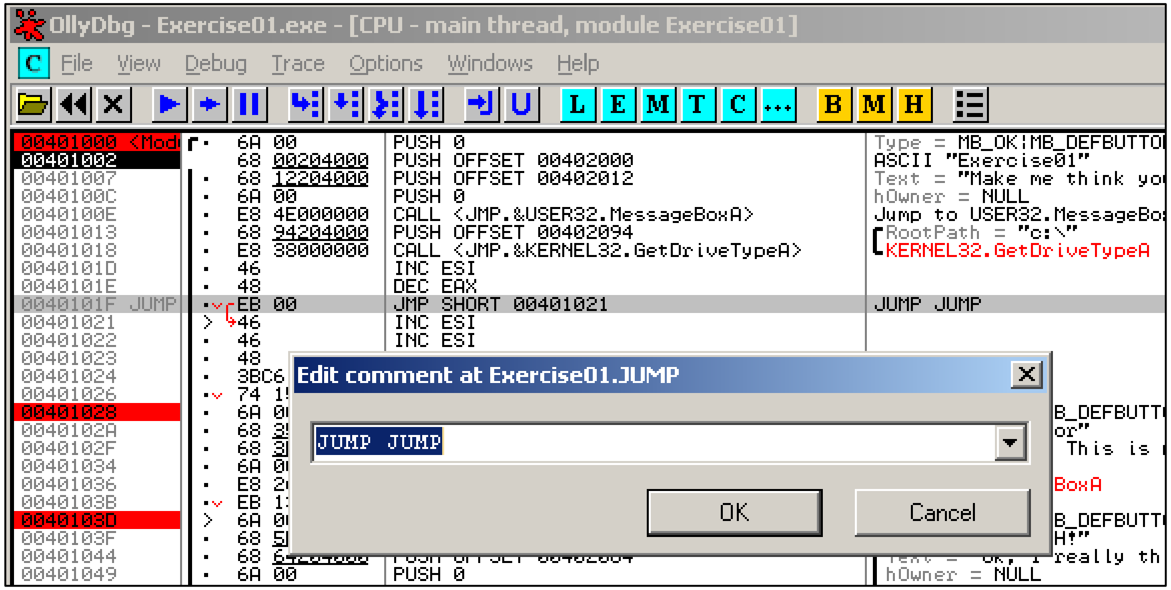
JUMP



```
00401000 <Modu ┌.  6A 00          PUSH 0                                Type = MB_OK|MB_DEFBUTTO
00401002        .  68 00204000    PUSH OFFSET 00402000                  ASCII "Exercise01"
00401007       |.  68 12204000    PUSH OFFSET 00402012                  Text = "Make me think yo
0040100C       |.  6A 00          PUSH 0                                hOwner = NULL
0040100E       |.  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>        Jump to USER32.MessageBo
00401013       |.  68 94204000    PUSH OFFSET 00402094                 ┌RootPath = "c:\"
00401018       |.  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>   └KERNEL32.GetDriveTypeA
0040101D       |.  46             INC ESI
0040101E       |.  48             DEC EAX
0040101F JUMP  |.v┌EB 00          JMP SHORT 00401021
00401021       |> └46             INC ESI
00401022       |.  46             INC ESI
00401023       |.  48             DEC EAX
```

OllyDbg

- **Add Comment – ‘;’**



OllyDbg - Exercise01.exe - [CPU - main thread, module Exercise01]
C File View Debug Trace Options Windows Help
L E M T C ... B M H

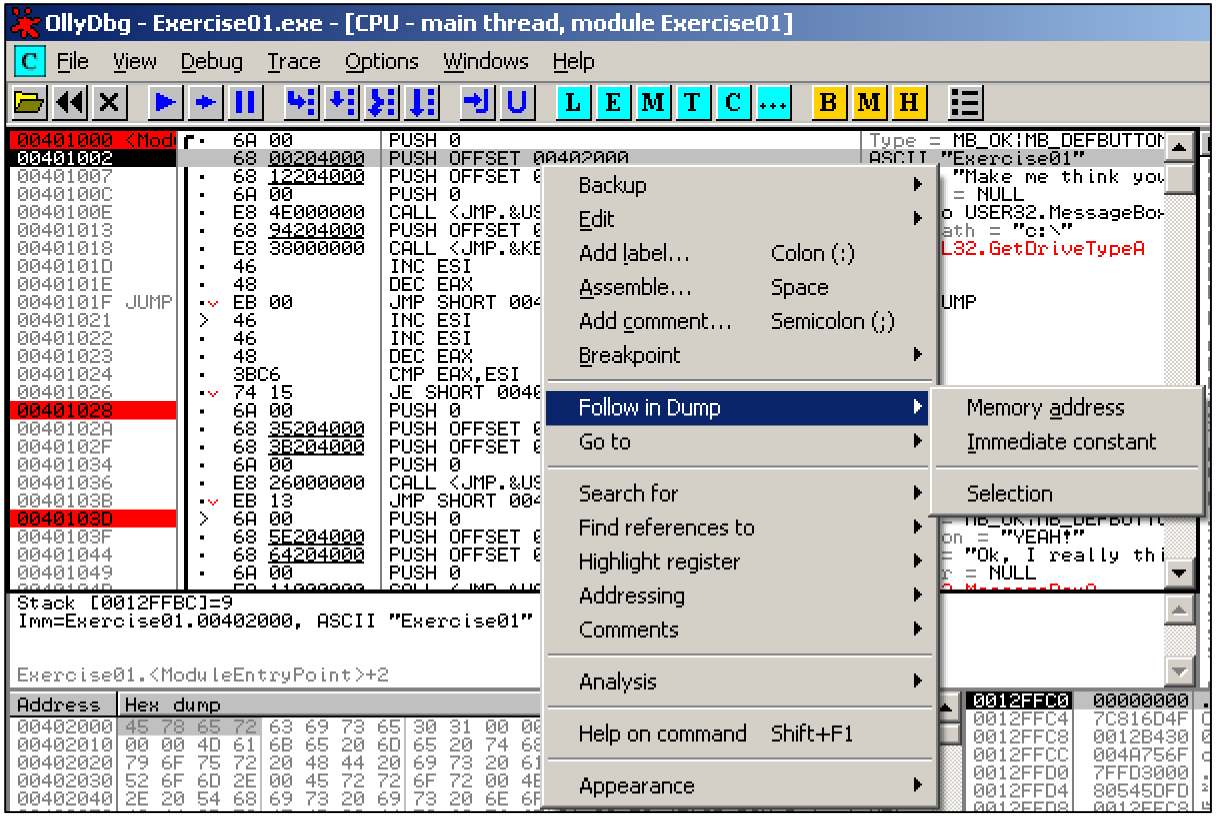
```
00401000 <Modu  6A 00         PUSH 0                              Type = MB_OK|MB_DEFBUTTO
00401002        68 00204000   PUSH OFFSET 00402000                ASCII "Exercise01"
00401007        68 12204000   PUSH OFFSET 00402012                Text = "Make me think yo
0040100C        6A 00         PUSH 0                              hOwner = NULL
0040100E        E8 4E000000   CALL <JMP.&USER32.MessageBoxA>      Jump to USER32.MessageBo
00401013        68 94204000   PUSH OFFSET 00402094                [RootPath = "c:\"
00401018        E8 38000000   CALL <JMP.&KERNEL32.GetDriveTypeA>  KERNEL32.GetDriveTypeA
0040101D        46            INC ESI
0040101E        48            DEC EAX
0040101F JUMP   EB 00         JMP SHORT 00401021                  JUMP JUMP
00401021        46            INC ESI
00401022        46            INC ESI
00401023        48
00401024        3BC6
00401026        74 1
00401028        6A 0                                               B_DEFBUTT
0040102A        68 3                                               or"
0040102F        68 3                                                This is
00401034        6A 0
00401036        E8 2                                               BoxA
0040103B        EB 1
0040103D        6A 0                                               B_DEFBUTT
0040103F        68 5                                               H!"
00401044        68                                                 really th
00401049        6A 00         PUSH 0                              hOwner = NULL
```

Edit comment at Exercise01.JUMP

JUMP JUMP

OllyDbg

- **Follow in Dump**
  - Immediate Constant, Selection



```
00401000 <Modu ┌.  6A 00         PUSH 0                 Type = MB_OK|MB_DEFBUTTON
00401002           68 00204000   PUSH OFFSET 00402000   ASCII "Exercise01"
00401007        .  68 12204000   PUSH OFFSET 0            "Make me think you
0040100C        .  6A 00         PUSH 0                   = NULL
0040100E        .  E8 4E000000   CALL <JMP.&US           o USER32.MessageBox
00401013        .  68 94204000   PUSH OFFSET 0           ath = "c:\"
00401018        .  E8 38000000   CALL <JMP.&KE           L32.GetDriveTypeA
0040101D        .  46            INC ESI
0040101E        .  48            DEC EAX
0040101F JUMP   .v EB 00         JMP SHORT 004           UMP
00401021        >  46            INC ESI
00401022        .  46            INC ESI
00401023        .  48            DEC EAX
00401024        .  3BC6          CMP EAX,ESI
00401026        .v 74 15         JE SHORT 0040
00401028        .  6A 00         PUSH 0
0040102A        .  68 35204000   PUSH OFFSET 0
0040102F        .  68 3B204000   PUSH OFFSET 0
00401034        .  6A 00         PUSH 0
00401036        .  E8 26000000   CALL <JMP.&US
0040103B        .v EB 13         JMP SHORT 004
0040103D        >  6A 00         PUSH 0                  on = "YEAH!"
0040103F        .  68 5E204000   PUSH OFFSET 0           = "Ok, I really thi
00401044        .  68 64204000   PUSH OFFSET 0           r = NULL
00401049        .  6A 00         PUSH 0
```

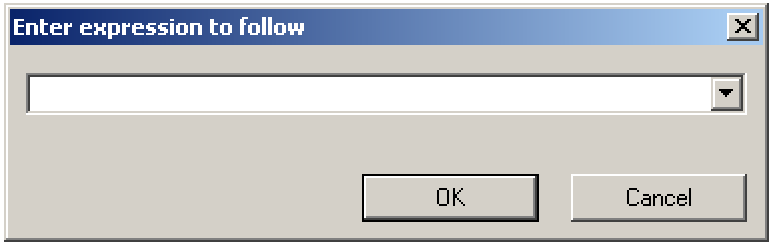
```
Stack [0012FFBC]=9
Imm=Exercise01.00402000, ASCII "Exercise01"

Exercise01.<ModuleEntryPoint>+2
```

```
Address  Hex dump
00402000 45 78 65 72 63 69 73 65 30 31 00 00
00402010 00 00 4D 61 6B 65 20 6D 65 20 74 68
00402020 79 6F 75 72 20 48 44 20 69 73 20 61
00402030 52 6F 6D 2E 00 45 72 72 6F 72 00 4E
00402040 2E 20 54 68 69 73 20 69 73 20 6E 6F
```

```
0012FFC0  00000000
0012FFC4  7C816D4F
0012FFC8  0012B430
0012FFCC  004A756F
0012FFD0  7FFD3000
0012FFD4  80545DFD
```

OllyDbg

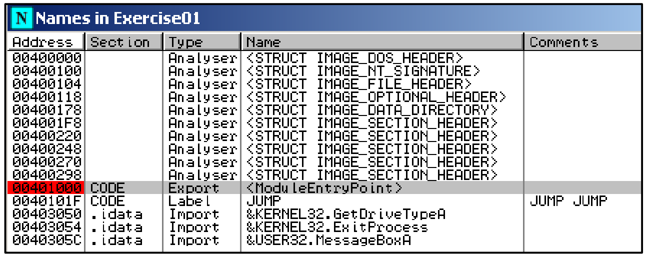
- **Go to**
  - Origin -‘*’
  - Expression -‘Ctrl + G’
  - Previous location -‘Minus’
  - Next location -‘Plus’
  - Previous procedure -‘Ctrl + Minus’
  - Next procedure -‘Ctrl + Plus’



Enter expression to follow

OllyDbg

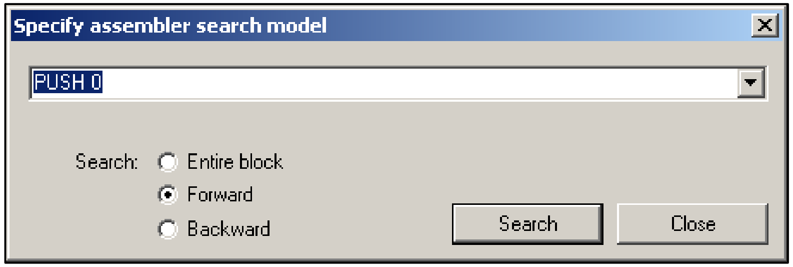
- **Search for**
  - Names -‘Ctrl + N’



Names in Exercise01

Address	Section	Type	Name	Comments
00400000		Analyser	<STRUCT IMAGE_DOS_HEADER>	
00400100		Analyser	<STRUCT IMAGE_NT_SIGNATURE>	
00400104		Analyser	<STRUCT IMAGE_FILE_HEADER>	
00400118		Analyser	<STRUCT IMAGE_OPTIONAL_HEADER>	
00400178		Analyser	<STRUCT IMAGE_DATA_DIRECTORY>	
004001F8		Analyser	<STRUCT IMAGE_SECTION_HEADER>	
00400220		Analyser	<STRUCT IMAGE_SECTION_HEADER>	
00400248		Analyser	<STRUCT IMAGE_SECTION_HEADER>	
00400270		Analyser	<STRUCT IMAGE_SECTION_HEADER>	
00400298		Analyser	<STRUCT IMAGE_SECTION_HEADER>	
00401000	CODE	Export	<ModuleEntryPoint>	
0040101F	CODE	Label	JUMP	JUMP JUMP
00403050	.idata	Import	&KERNEL32.GetDriveTypeA	
00403054	.idata	Import	&KERNEL32.ExitProcess	
0040305C	.idata	Import	&USER32.MessageBoxA	

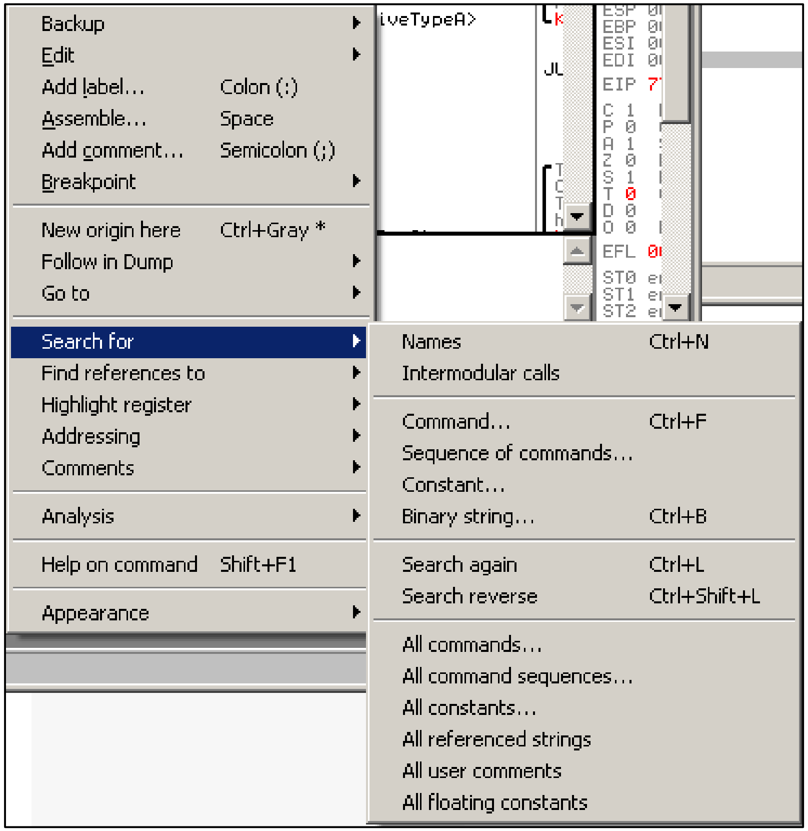
  - Command -‘Ctrl + F’



Specify assembler search model

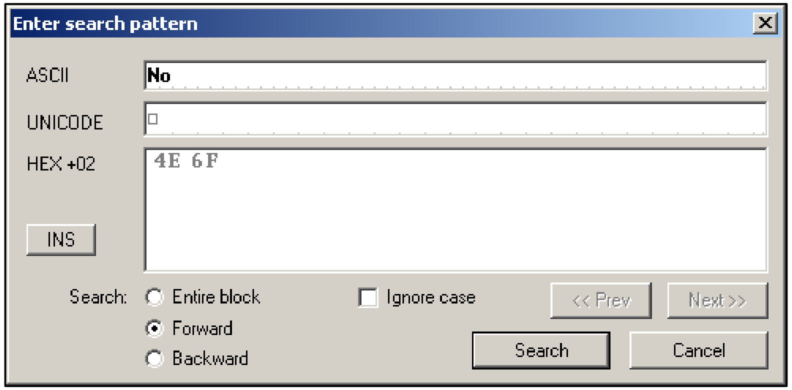
PUSH 0

Search: ○ Entire block ● Forward ○ Backward



OllyDbg

- **Search for**
  - Binary string -‘Ctrl + B’



Enter search pattern

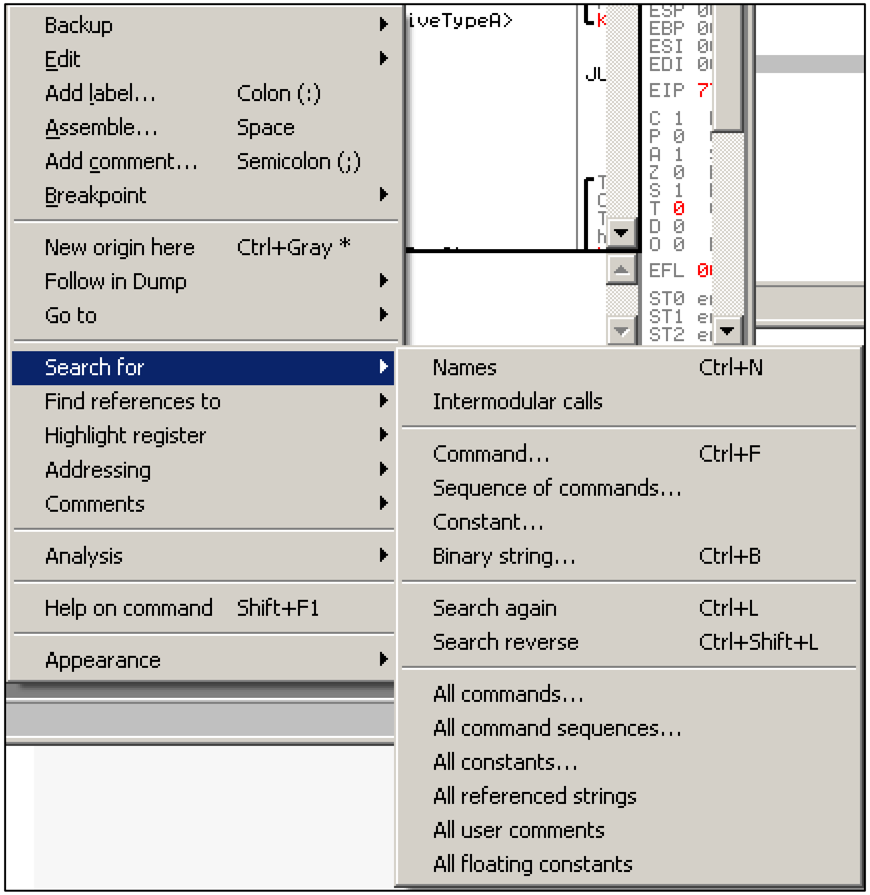
ASCII: No

UNICODE: □

HEX +02: 4E 6F

Search: ○ Entire block ● Forward ○ Backward

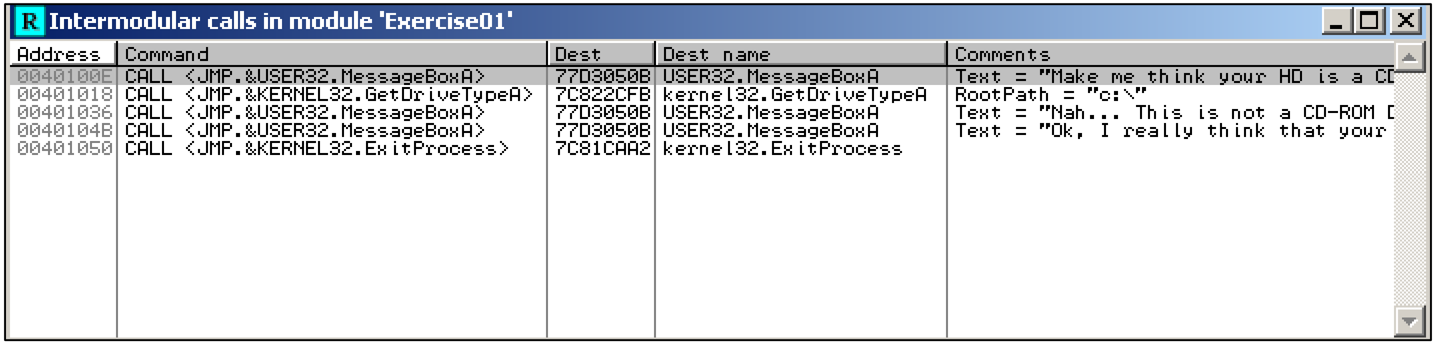
□ Ignore case



  - Search again -‘Ctrl + L’
  - Search reverse -‘Ctrl + Shift + L’

OllyDbg

- **Search for**
  - Intermodularcalls

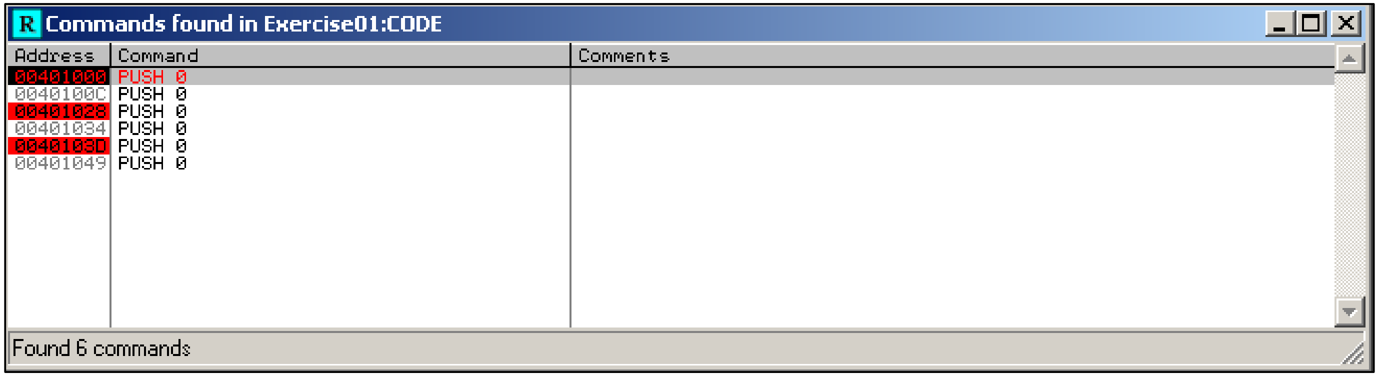


Intermodular calls in module 'Exercise01'

Address	Command	Dest	Dest name	Comments
0040100E	CALL <JMP.&USER32.MessageBoxA>	77D3050B	USER32.MessageBoxA	Text = "Make me think your HD is a CD
00401018	CALL <JMP.&KERNEL32.GetDriveTypeA>	7C822CFB	kernel32.GetDriveTypeA	RootPath = "c:\"
00401036	CALL <JMP.&USER32.MessageBoxA>	77D3050B	USER32.MessageBoxA	Text = "Nah... This is not a CD-ROM D
0040104B	CALL <JMP.&USER32.MessageBoxA>	77D3050B	USER32.MessageBoxA	Text = "Ok, I really think that your
00401050	CALL <JMP.&KERNEL32.ExitProcess>	7C81CAA2	kernel32.ExitProcess	

OllyDbg

- **Search for**
  - All commands

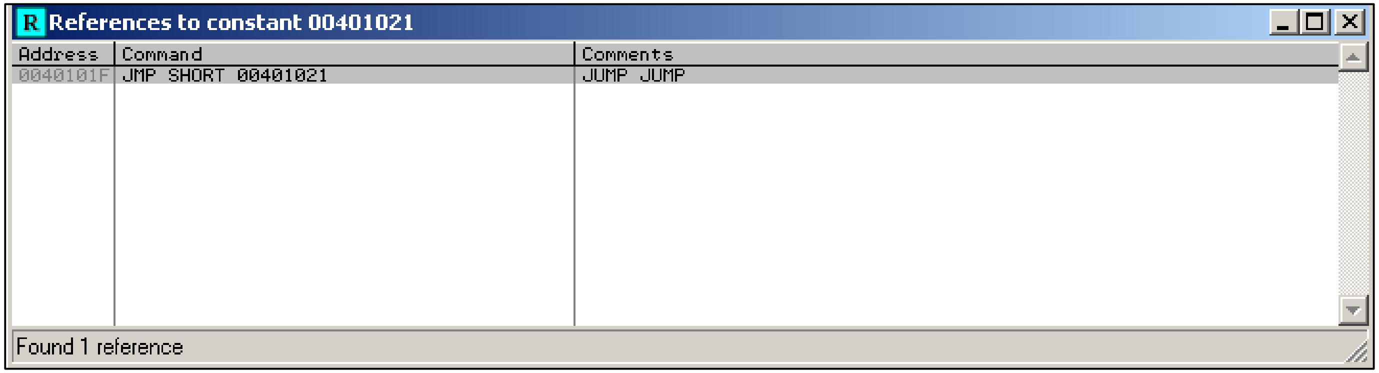


Commands found in Exercise01:CODE

```
Address   Command                    Comments
00401000  PUSH 0
0040100C  PUSH 0
00401028  PUSH 0
00401034  PUSH 0
0040103D  PUSH 0
00401049  PUSH 0
```

Found 6 commands

  - All constants



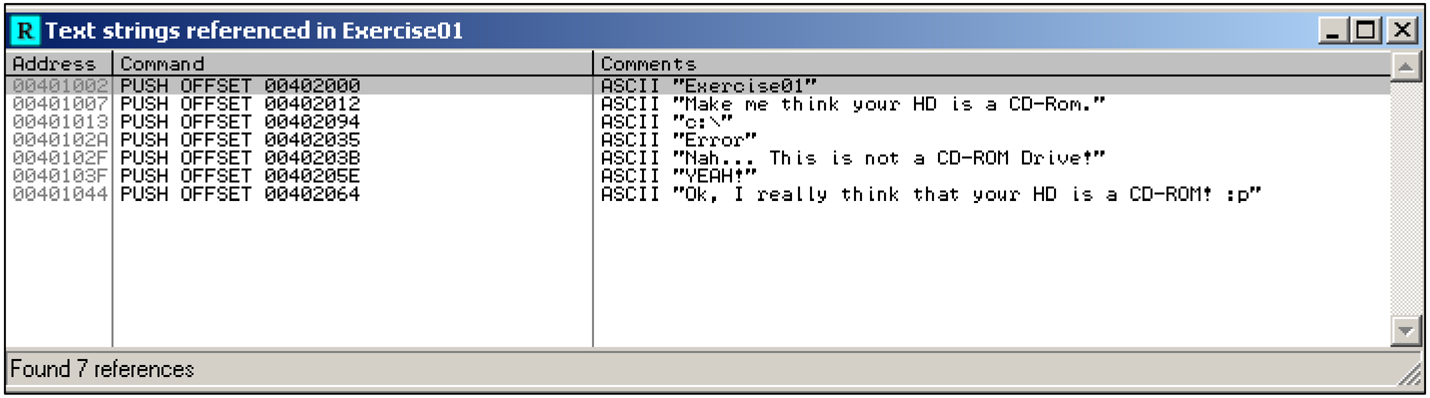
References to constant 00401021

```
Address   Command                    Comments
0040101F  JMP SHORT 00401021         JUMP JUMP
```

Found 1 reference

OllyDbg

- **Search for**
  - All referenced strings



```
Address  Command                Comments
00401002 PUSH OFFSET 00402000   ASCII "Exercise01"
00401007 PUSH OFFSET 00402012   ASCII "Make me think your HD is a CD-Rom."
00401013 PUSH OFFSET 00402094   ASCII "c:\"
0040102A PUSH OFFSET 00402035   ASCII "Error"
0040102F PUSH OFFSET 0040203B   ASCII "Nah... This is not a CD-ROM Drive!"
0040103F PUSH OFFSET 0040205E   ASCII "YEAH!"
00401044 PUSH OFFSET 00402064   ASCII "Ok, I really think that your HD is a CD-ROM! :p"
```

Found 7 references

Thank you for listening

koha@korea.ac.kr