
# Reverse engineering

# IDA

**Chanung Pak**

**koha@korea.ac.kr**

# IDA : Basic Usage

- **Created by Ilfak Guilfanov**

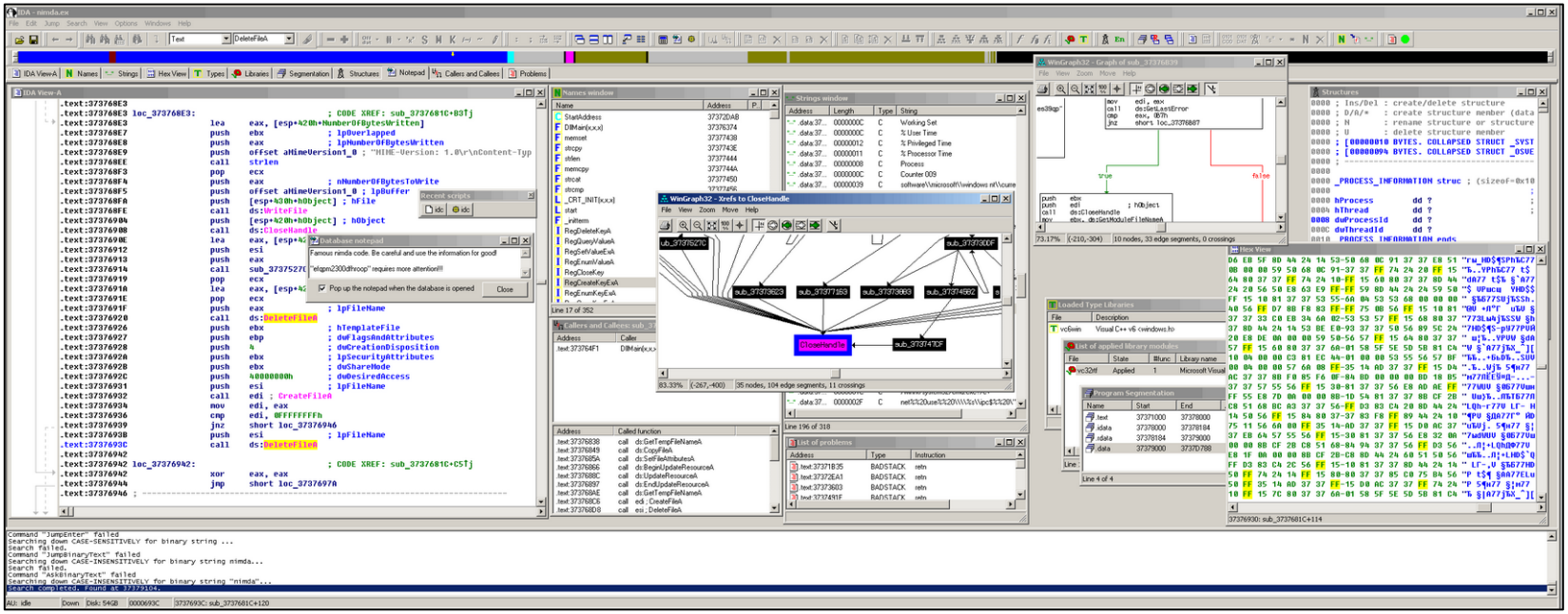
- **Founder and CEO of Hex-Rays**

- **Premier disassembly tool available today**
  - Interactive (IDCScript, IDAPython)
  - Many platforms supported (Multi-processor)
  - Highly extensible (Plug-in)

- **Related manual**
  - “The IDA Pro book” by Chris Eagle
  - “Reverse Engineering Code with IDA Pro” by Dan Kaminsky

# IDA : Basic Usage

- **IDA (Interactive DisAssembler)**
  - https://www.hex-rays.com/founded by IlfakGuilfanov
  - Two editions: IDA Professional, IDA Starter
- **IDA (Disassembler & Debugger) + Hex-Rays Decompiler**



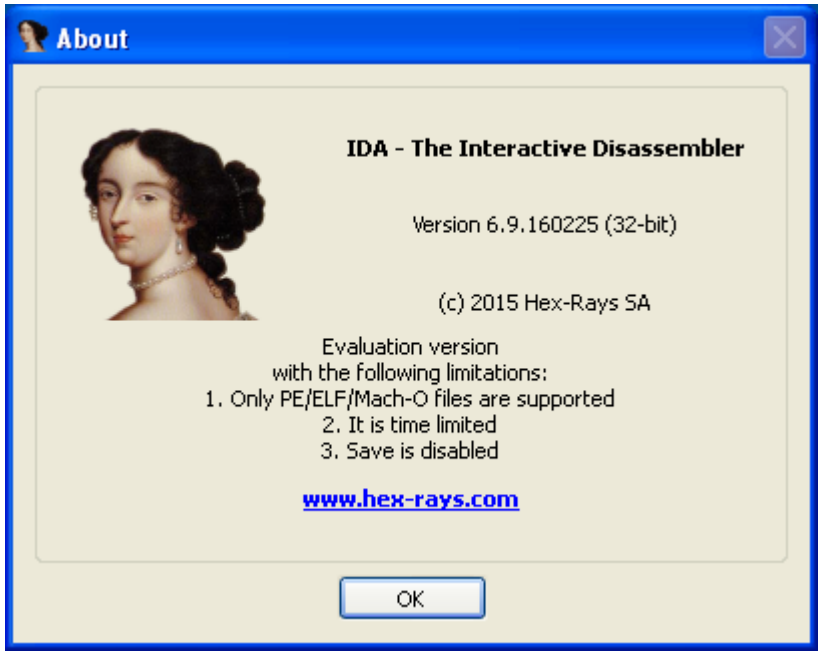
# IDA : Basic Usage

- **Key Features: Disassembler**
  - Supported processors https://www.hex-rays.com/products/ida/processors.shtml
  - Various executable file formats, Code graphing
  - SDK, Plug-in, IDC Script, IDAPython
- **Key Features: Debugger**

| Target Platform | IDA runs on Windows | IDA runs on Linux | IDA runs on Mac OS X | Notes |
|---|---|---|---|---|
| Windows 32/64 bits | Local/Remote | Remote | Remote | On 64 bits - remote only |
| Linux 32/64 bits | Remote | Local/Remote | Remote | |
| OS X 32/64 bits | Remote | Remote | Local/Remote | |
| Bochs | Bochs Emulator | Bochs Emulator | Bochs Emulator | |
| GDB Server | GDB Server | GDB Server | GDB Server | x86, ARM, PowerPC, MIPS |
| WinDBG 32/64 bits | Remote | - | - | User-mode, Kernel-mode |
| Android (Dalvik) | Remote | Remote | Remote | DEX bytecode, Source |

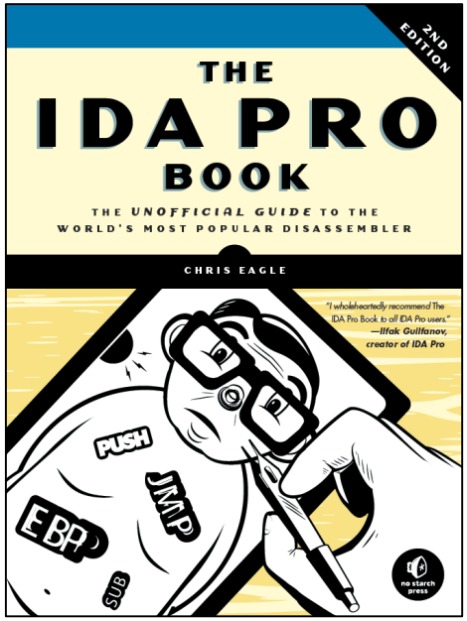
# IDA : Basic Usage

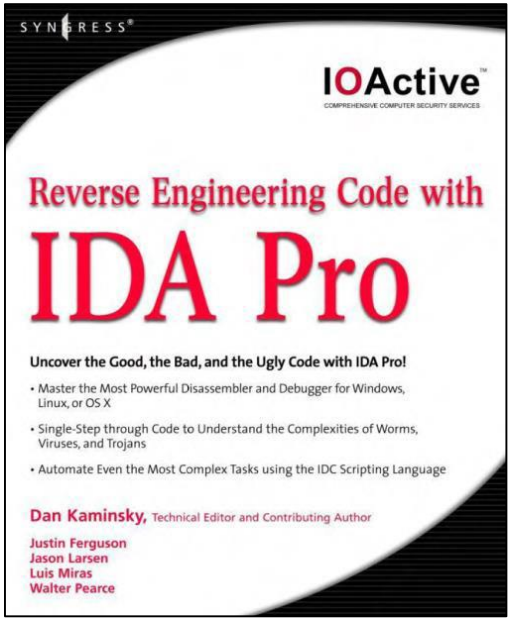
- **Evaluation & Freeware versions**
  - https://www.hex-rays.com/products/ida/support/download.shtml
  - Freeware: v5.0
  - Evaluation version v6.9
    - Only supports INTEL 80x86 & ARM family
    - Only supports PE/ELF/Mach-O formats
    - Time limited (30 min?)
    - Save is disabled



# IDA : Basic Usage

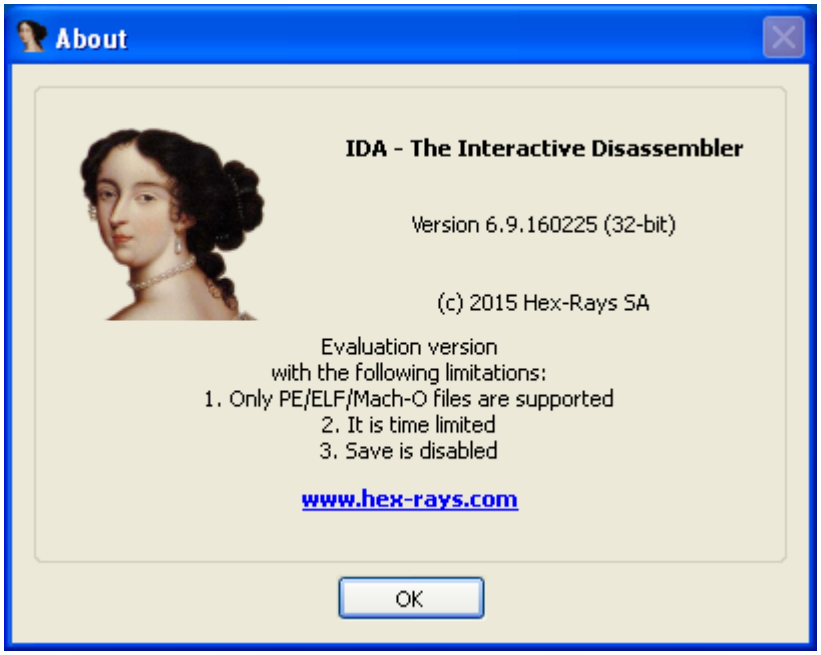
- **References**
  - “The IDA Pro Book 2nd Edition” by Chris Eagle
  - “Reverse Engineering Code with IDA Pro” by Dan Kaminsky
  - https://www.hex-rays.com/products/ida/support/idadoc/index.shtml
  - http://www.hexblog.com/

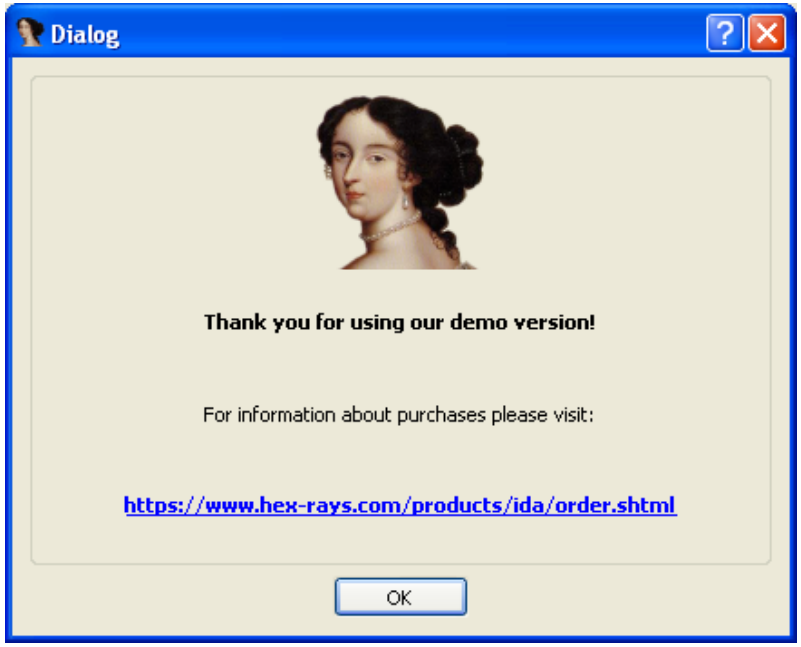



# IDA : Basic Usage

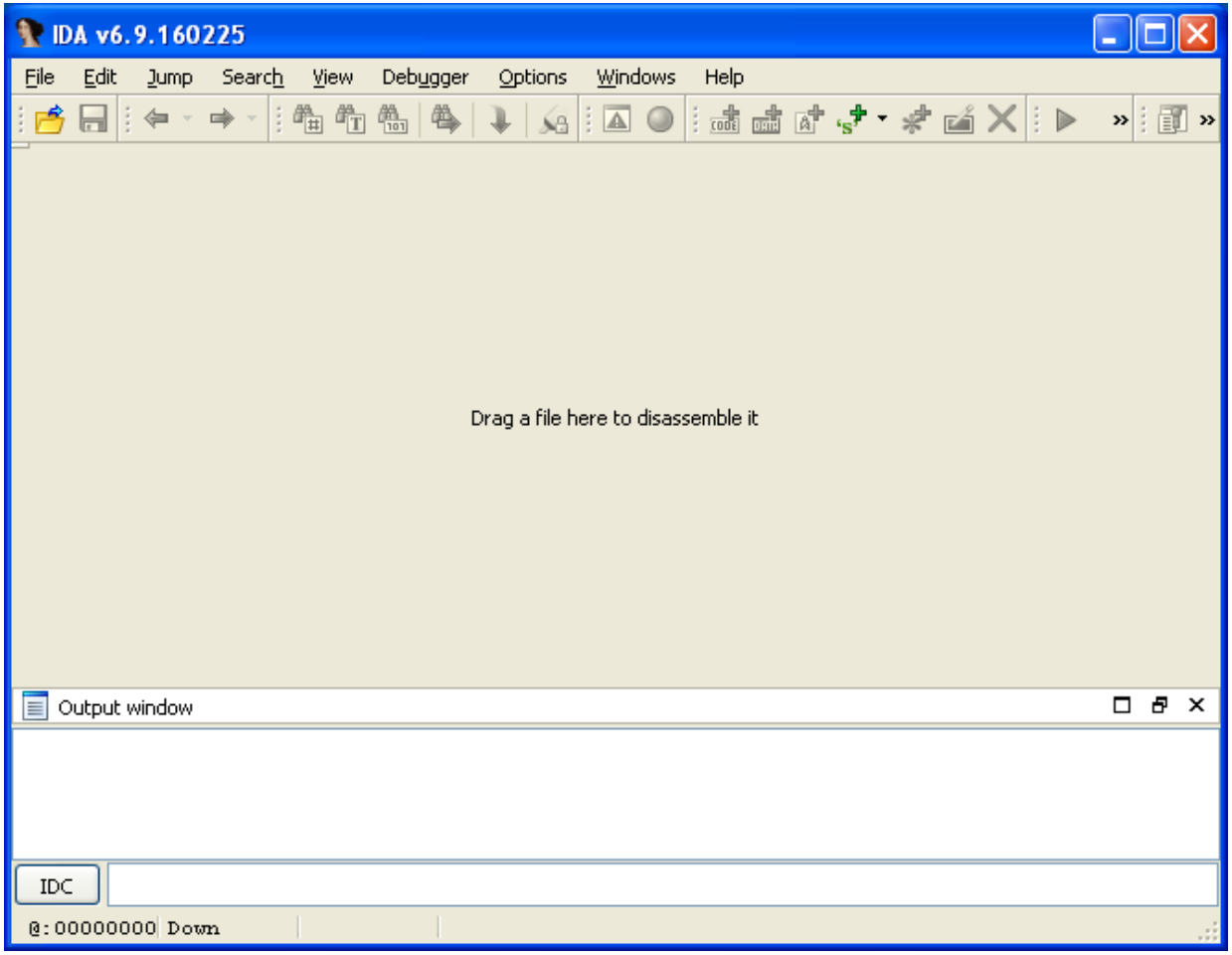
- **Launching IDA**

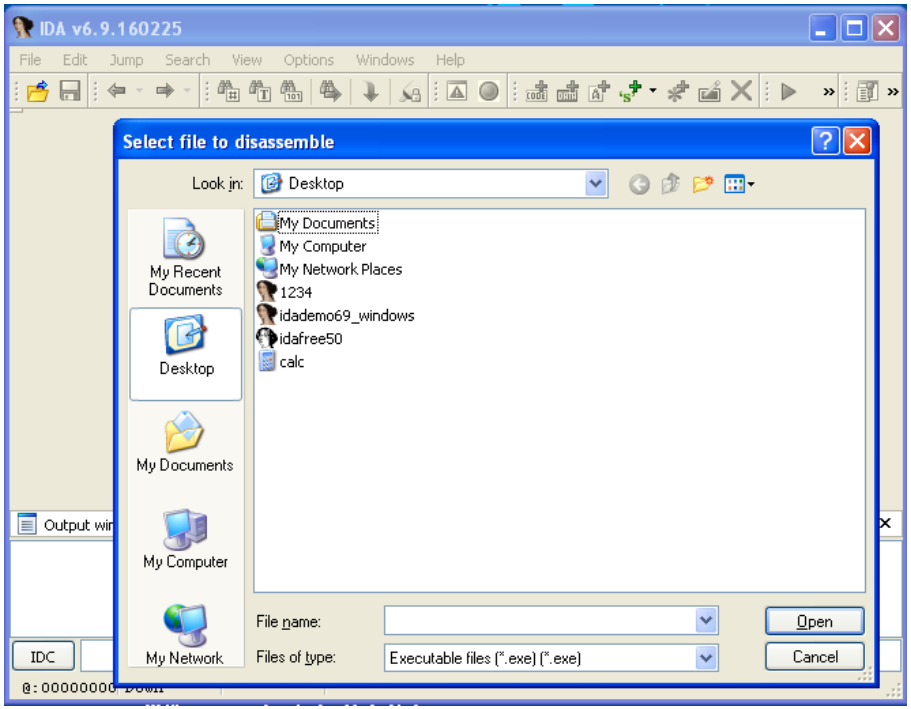
# IDA : Basic Usage

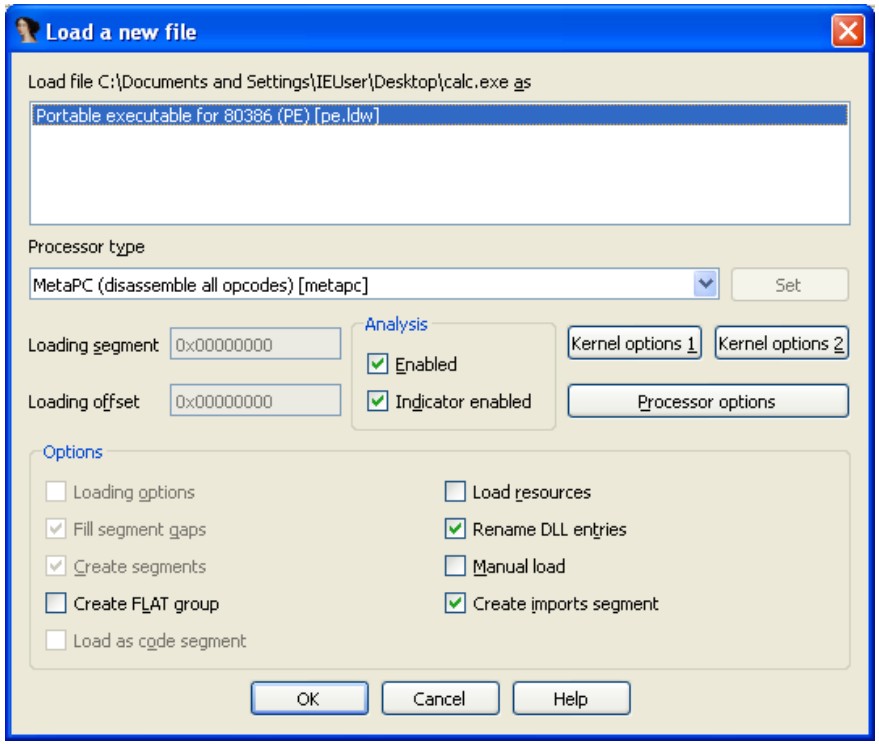
- **Launching IDA**



# IDA : Basic Usage

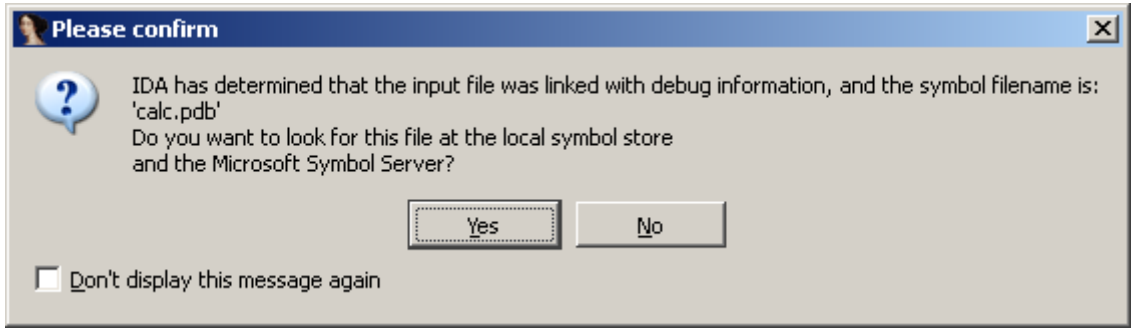
- **Launching IDA - Executable File**

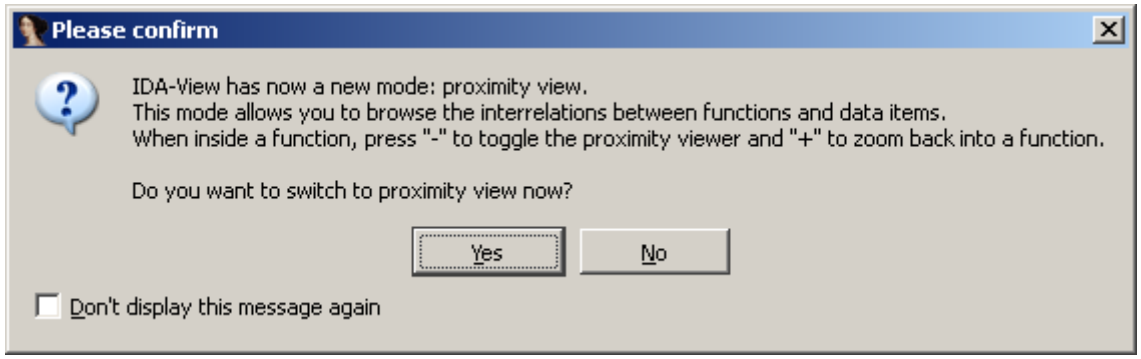


# IDA : Basic Usage

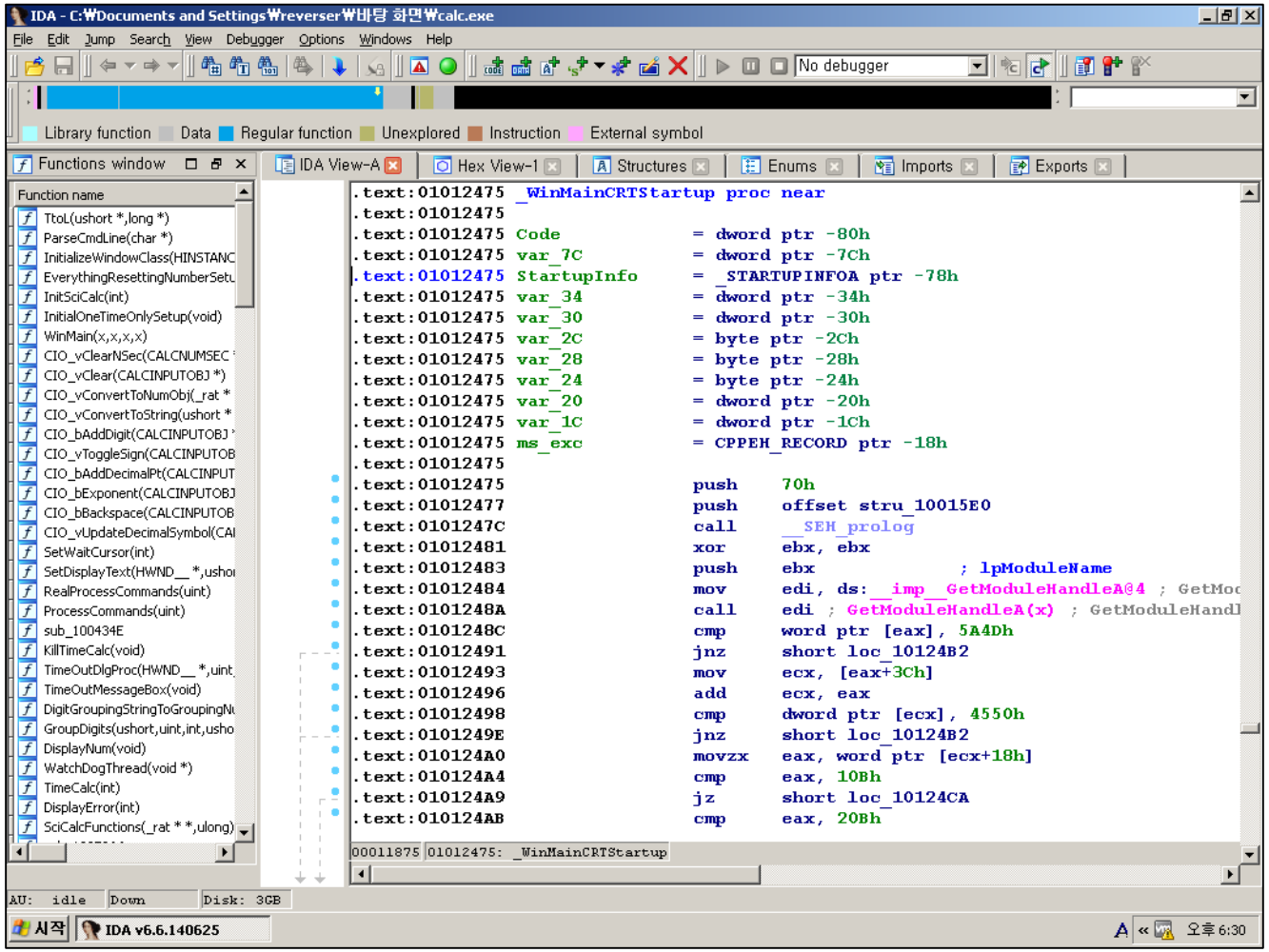
- **Launching IDA -Executable File**



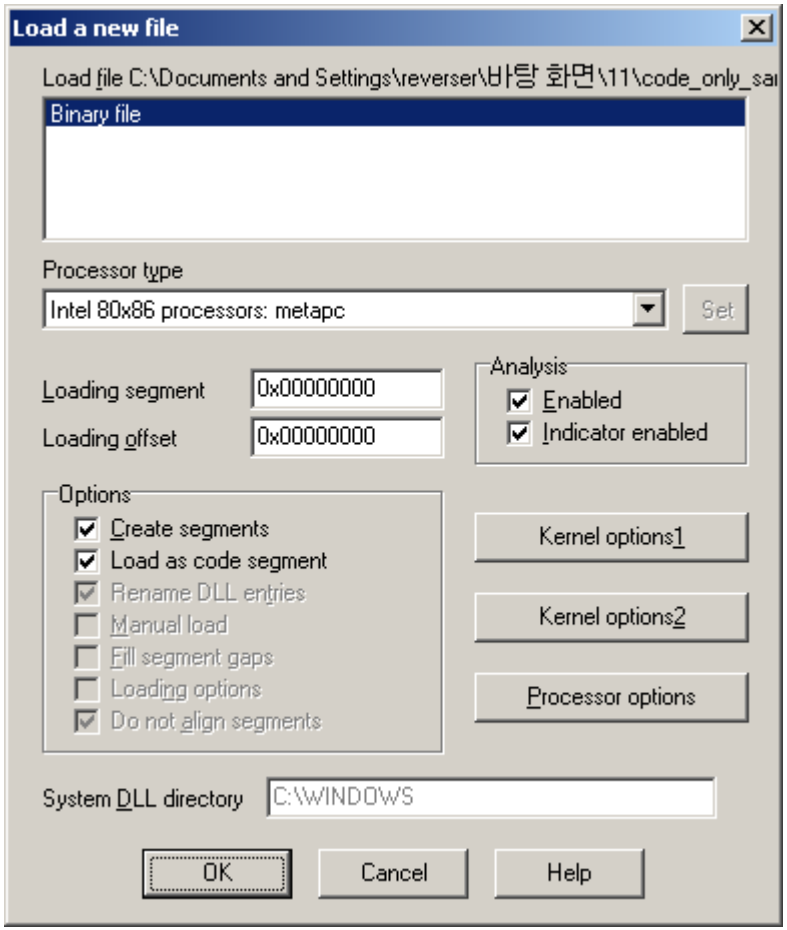
# IDA : Basic Usage

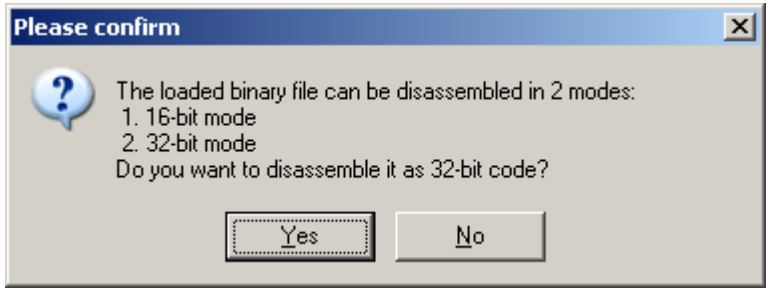
- **Launching IDA -Executable File**

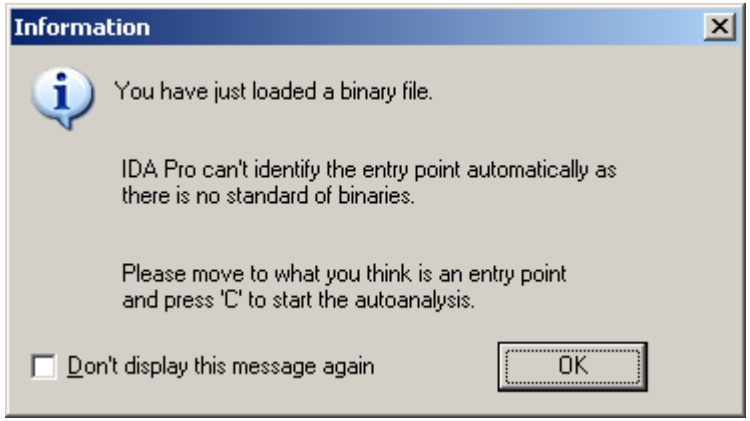


# IDA : Basic Usage

- **Launching IDA -Binary File**

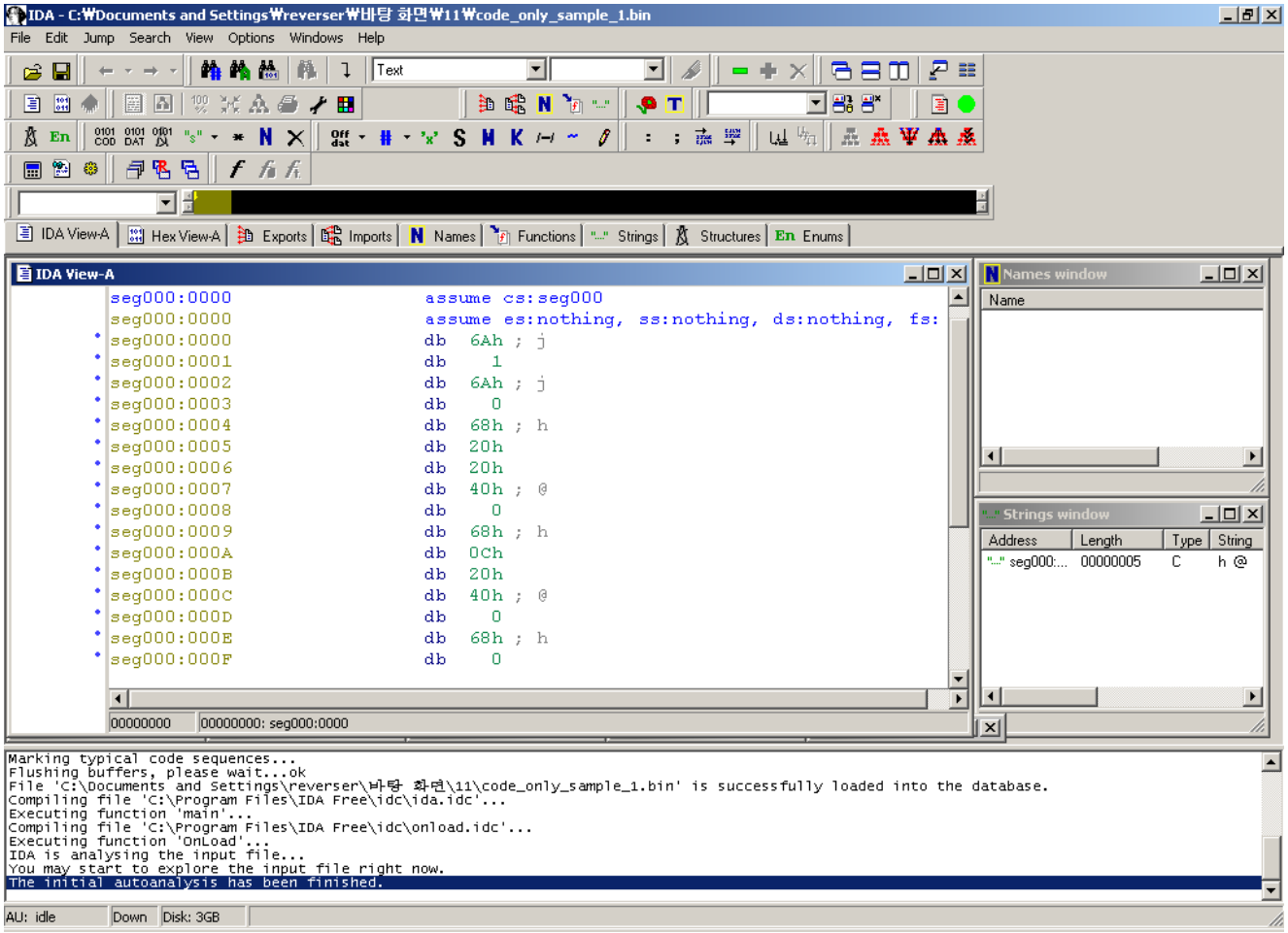


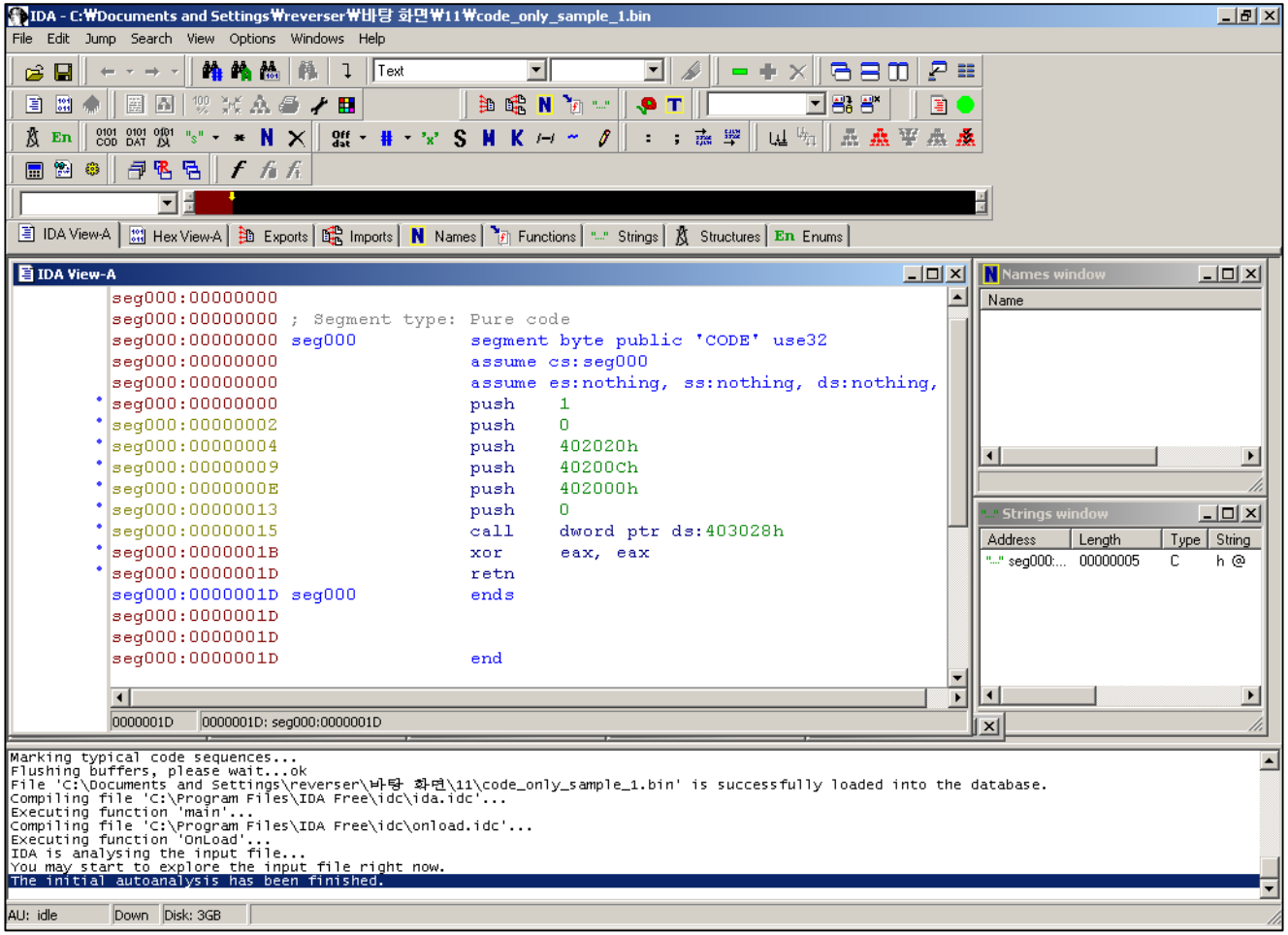
# IDA : Basic Usage

- **Launching IDA -Binary File**



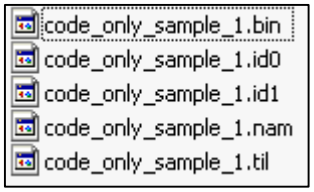
# IDA : Basic Usage

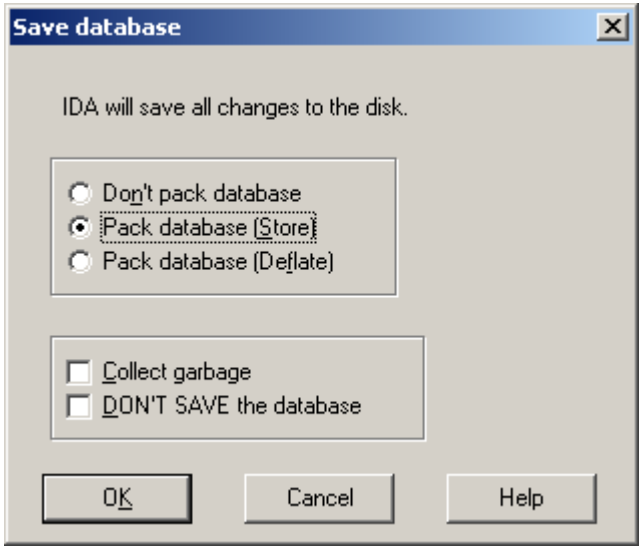
- **Launching IDA -Binary File**

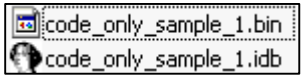


# IDA : Basic Usage

- **IDA Database Files**
  - 4 Components: id0, id1, nam, til
  - Hotkey - ‘ Ctrl + W ’
  - Pack file: idb (IDA Database)
  - Save options
    - Pack database –Store or Deflate
  - Lack of the ‘undo’ feature

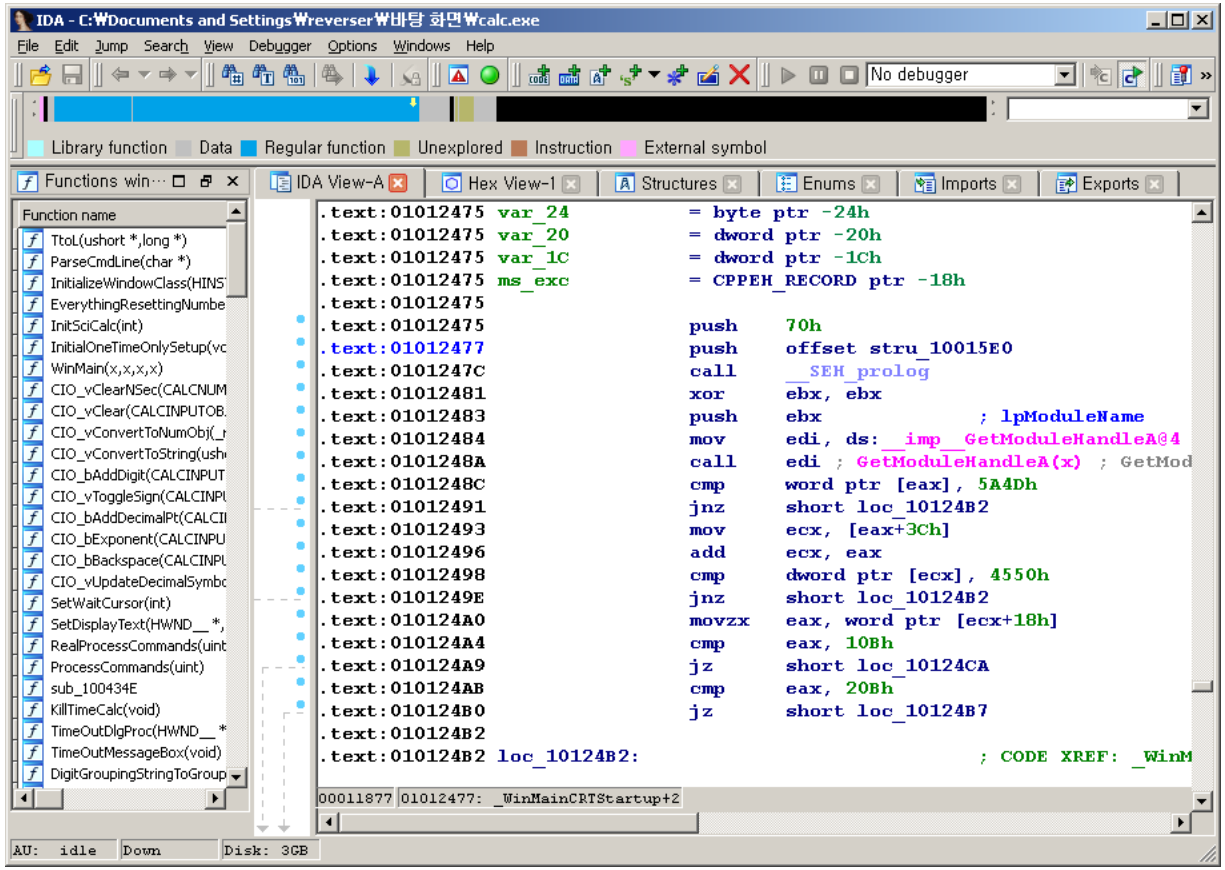


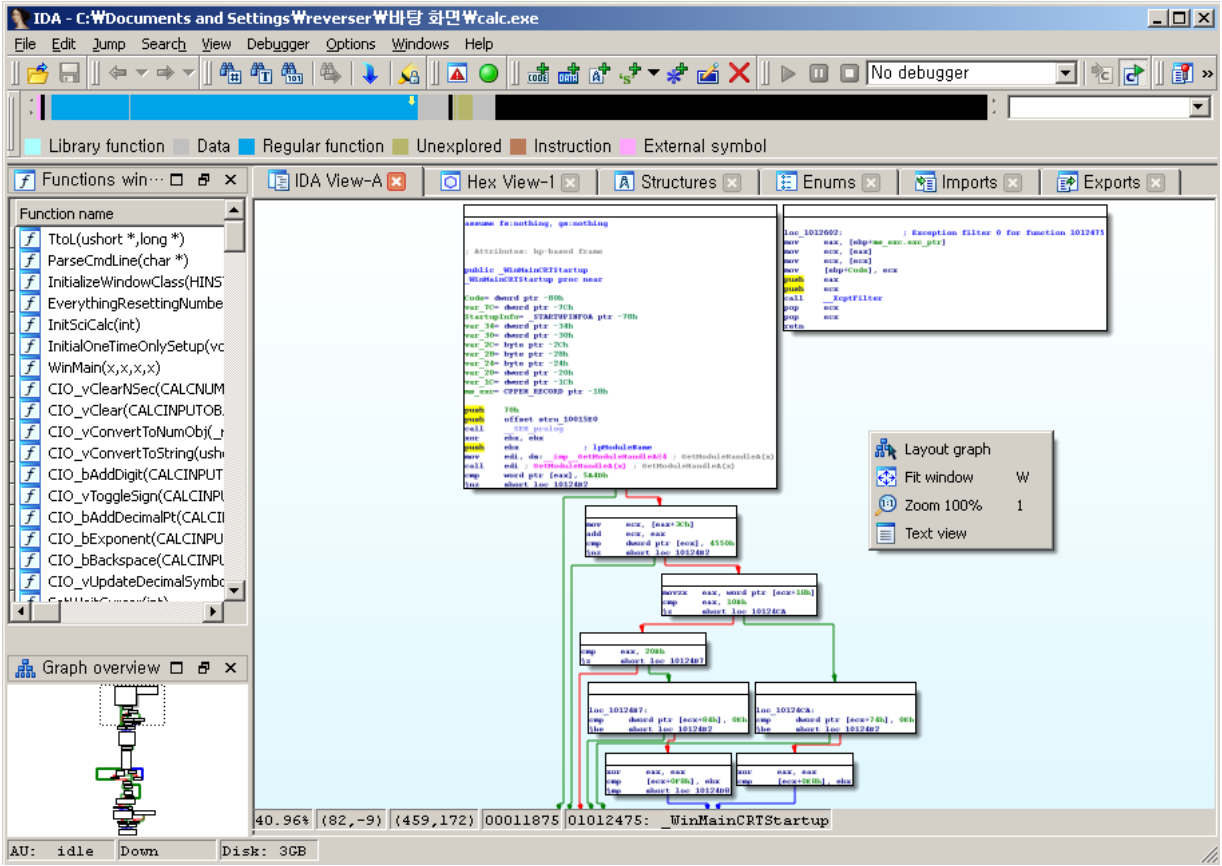
# IDA : Basic Usage

- **IDA Desktop**



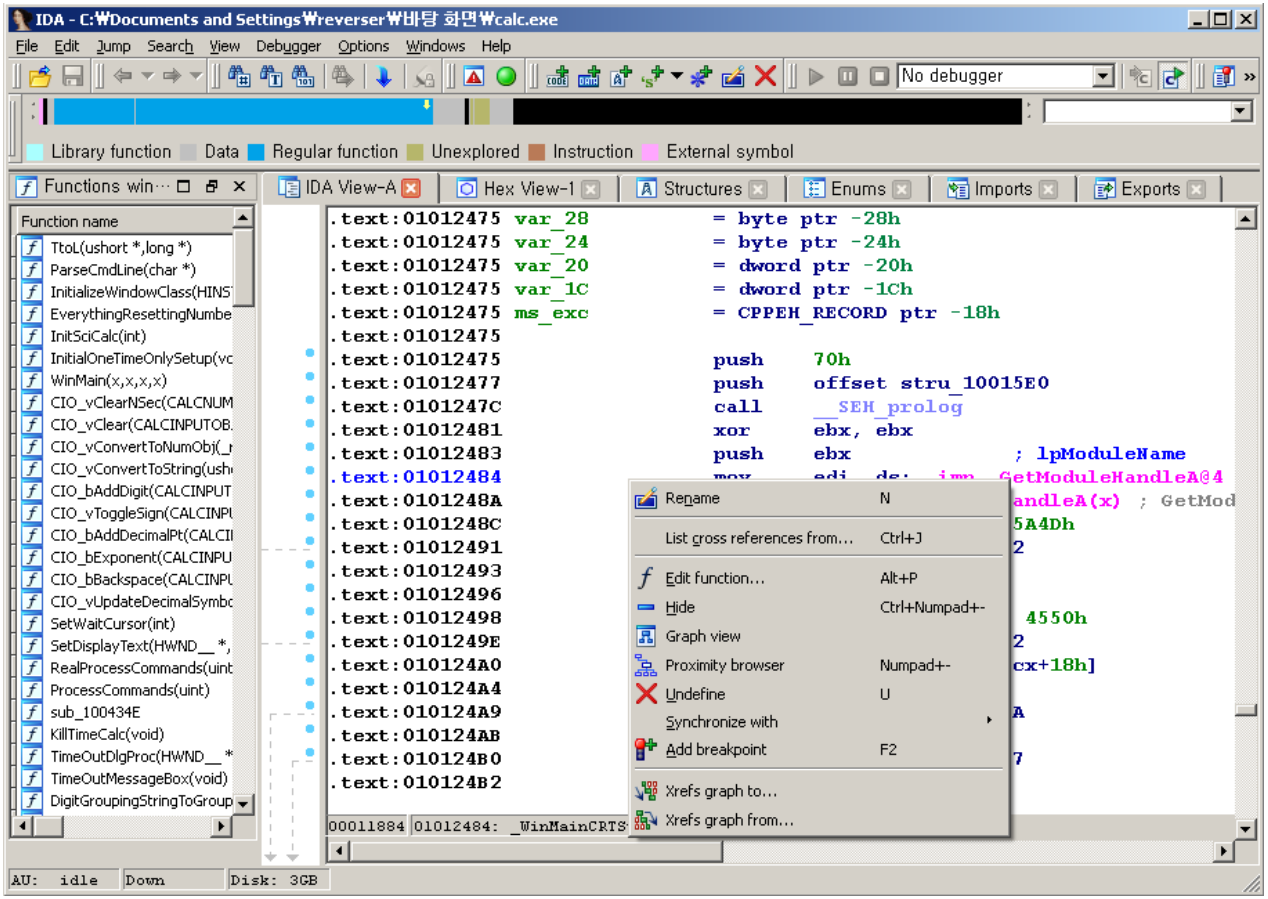
# IDA : Basic Usage

- **IDA View -Disassembly Window**
  - Graph view -‘Space bar’



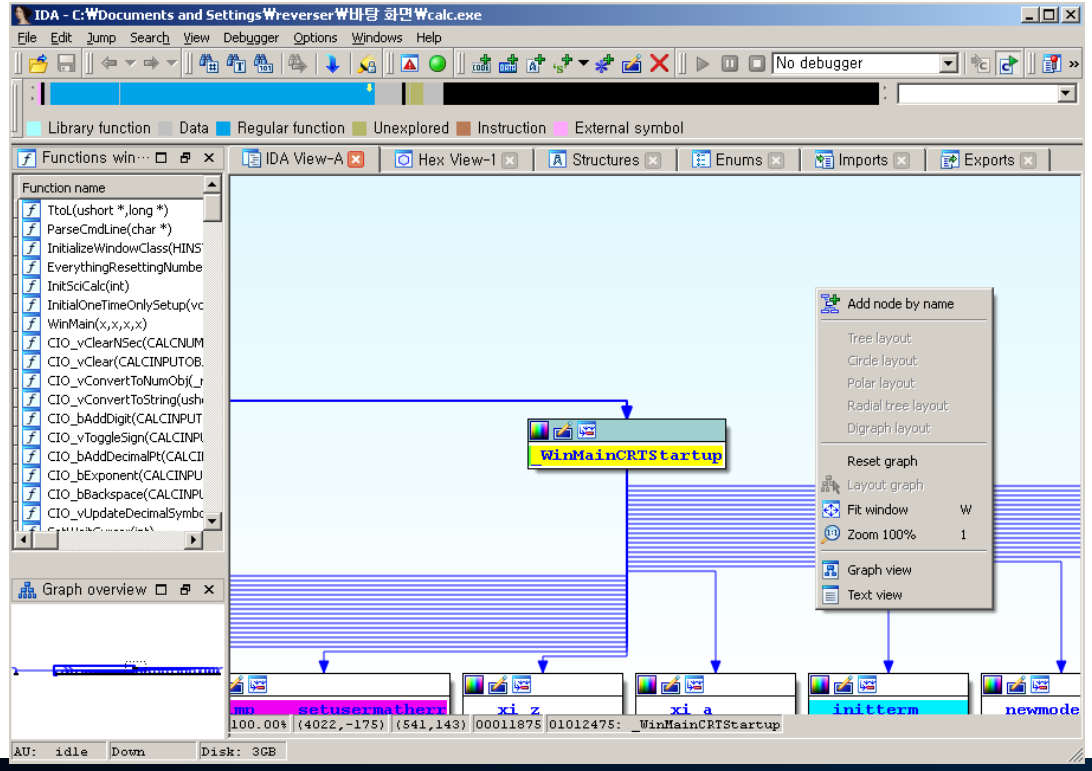
# IDA : Basic Usage

- **IDA View -Disassembly Window**
  - Text view-‘Space bar’



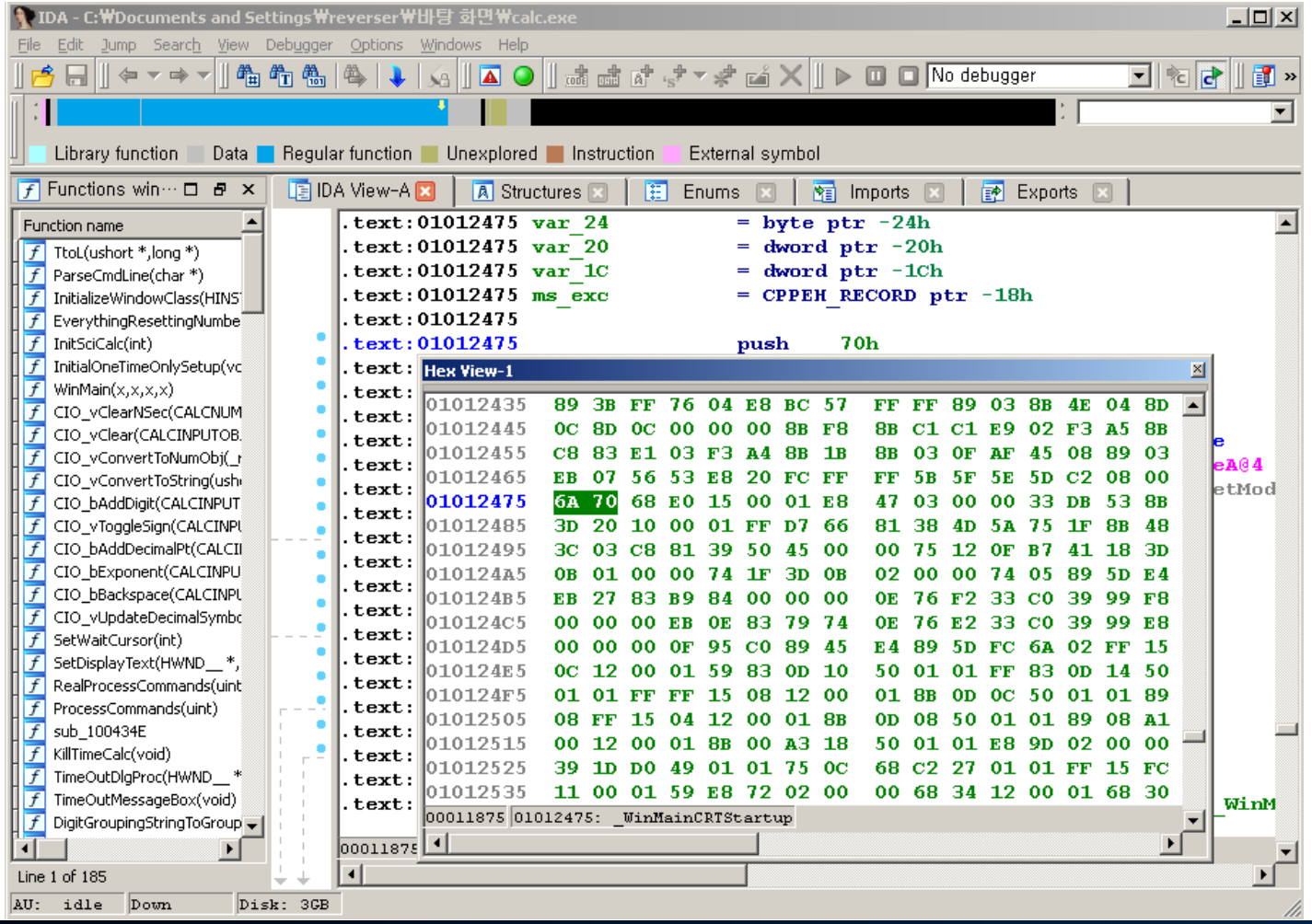
# IDA : Basic Usage

- **IDA View -Disassembly Window**
  - Proximity browser (from IDA v6.2) - ‘ - ’
    - Call graph of a Program
    - Supported layouts: Tree, Circle, Polar, Radial tree, Digraph



# IDA : Basic Usage

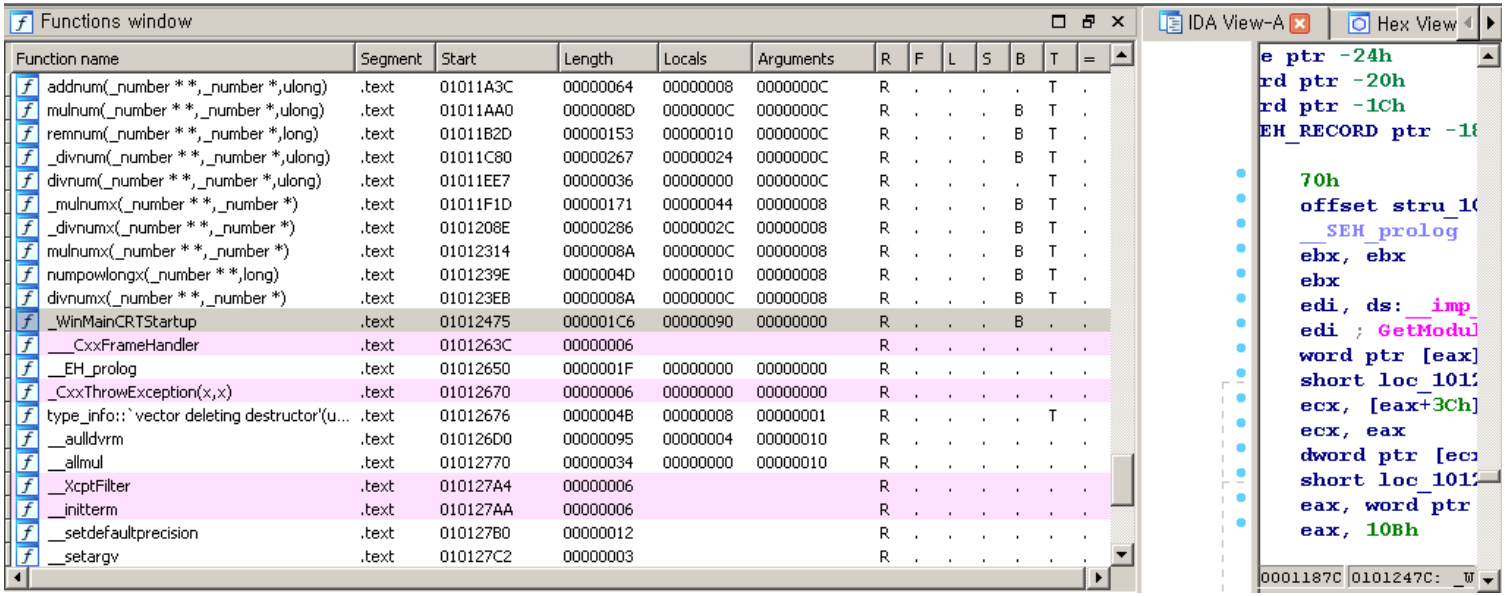
- **Hex View**



# IDA : Basic Usage

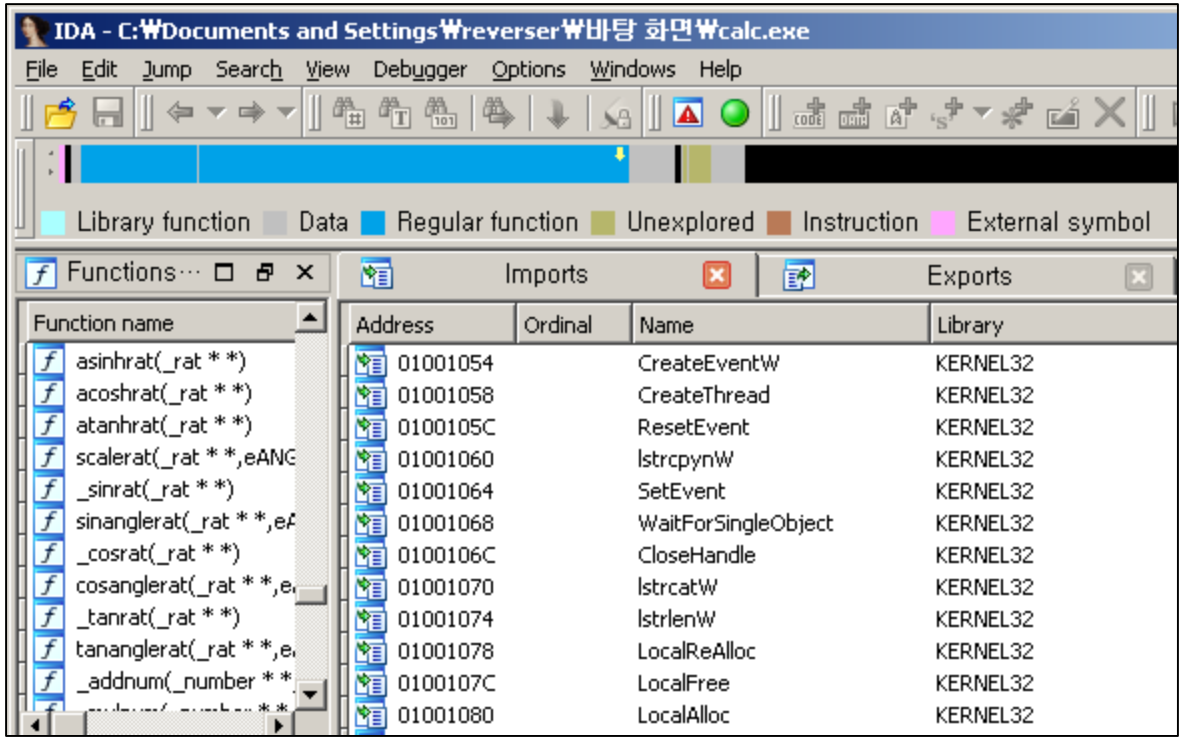
- **Functions Window**
  - ‘Shift + F3’

| Flag | Description |
|---|---|
| R | Function returns to caller |
| F | Far function |
| L | Library function |
| S | Static function |
| B | EBP based frame |
| T | Function has type information |
| = | Frame pointer is equal to the initial stack pointer |



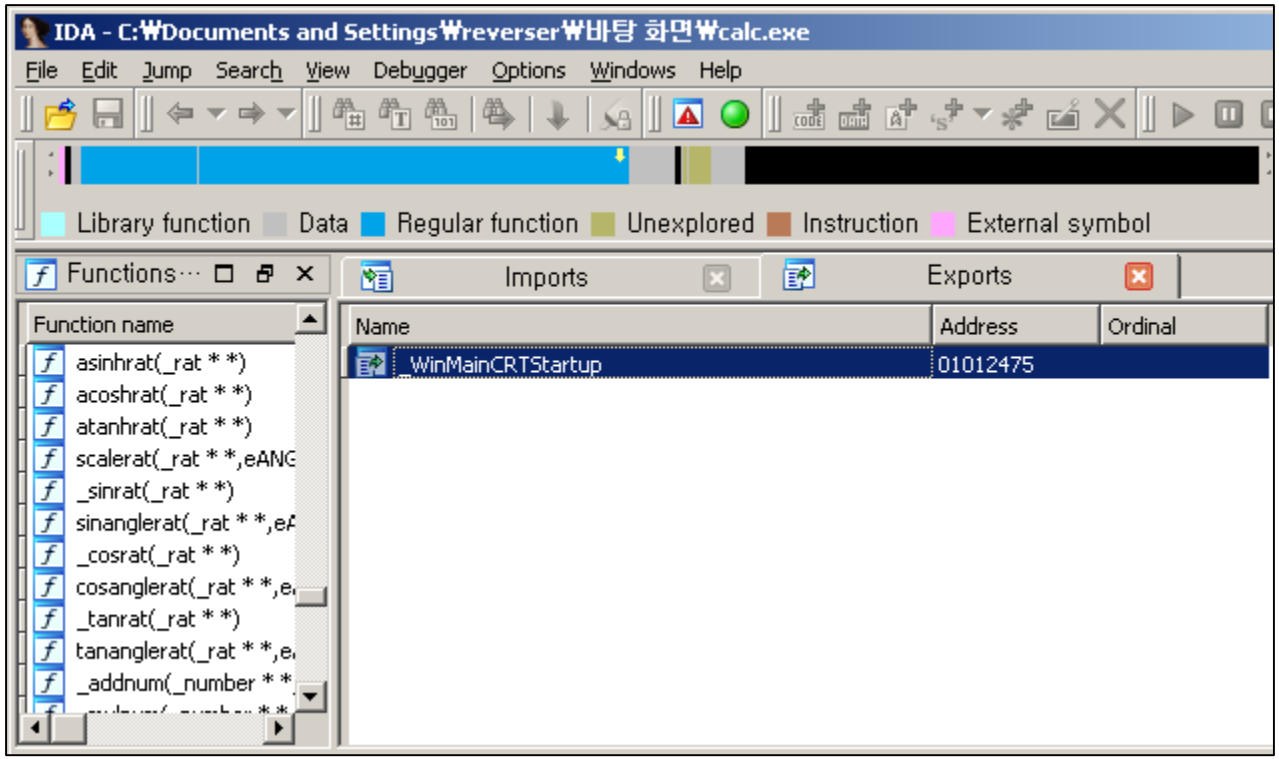
# IDA : Basic Usage

- **Imports Window**



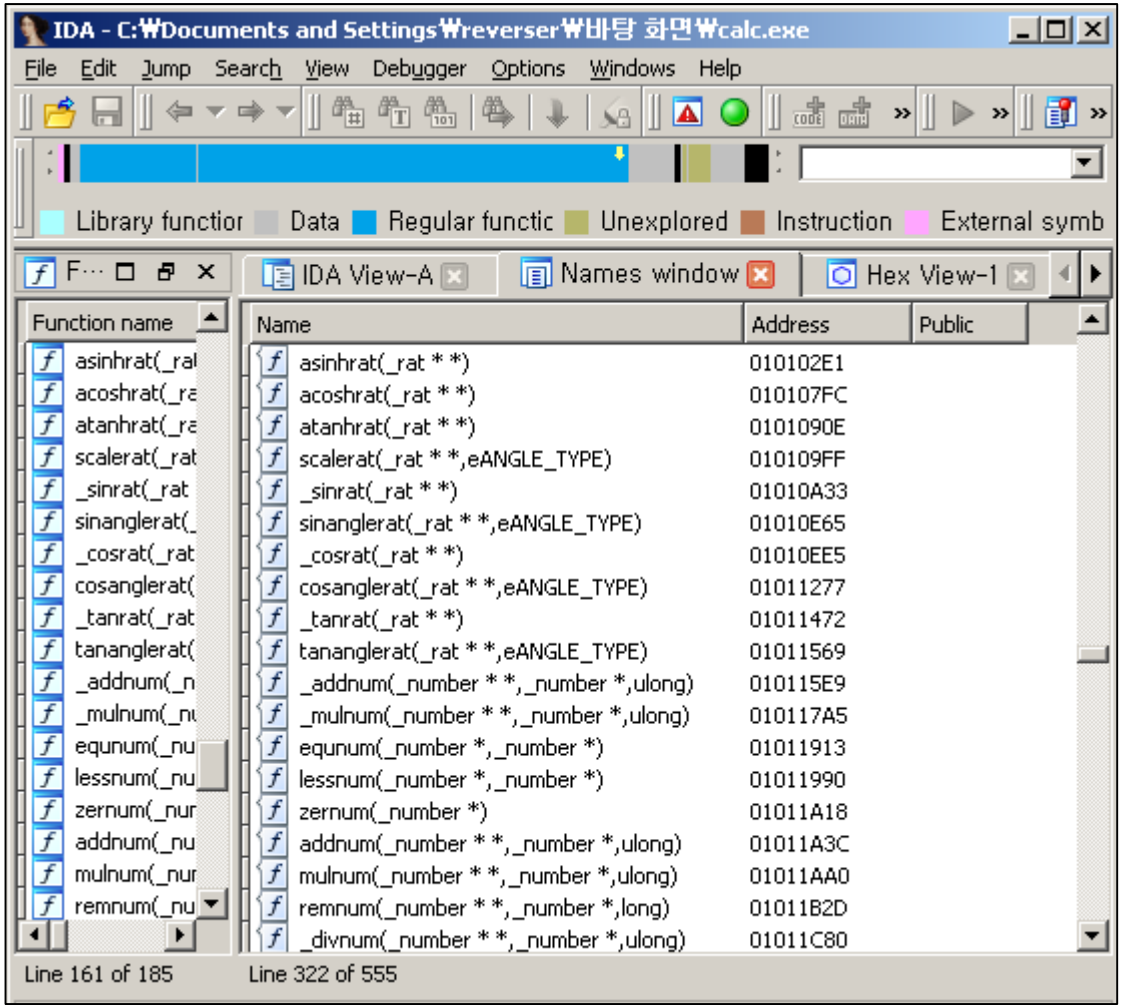
# IDA : Basic Usage

- **Exports**



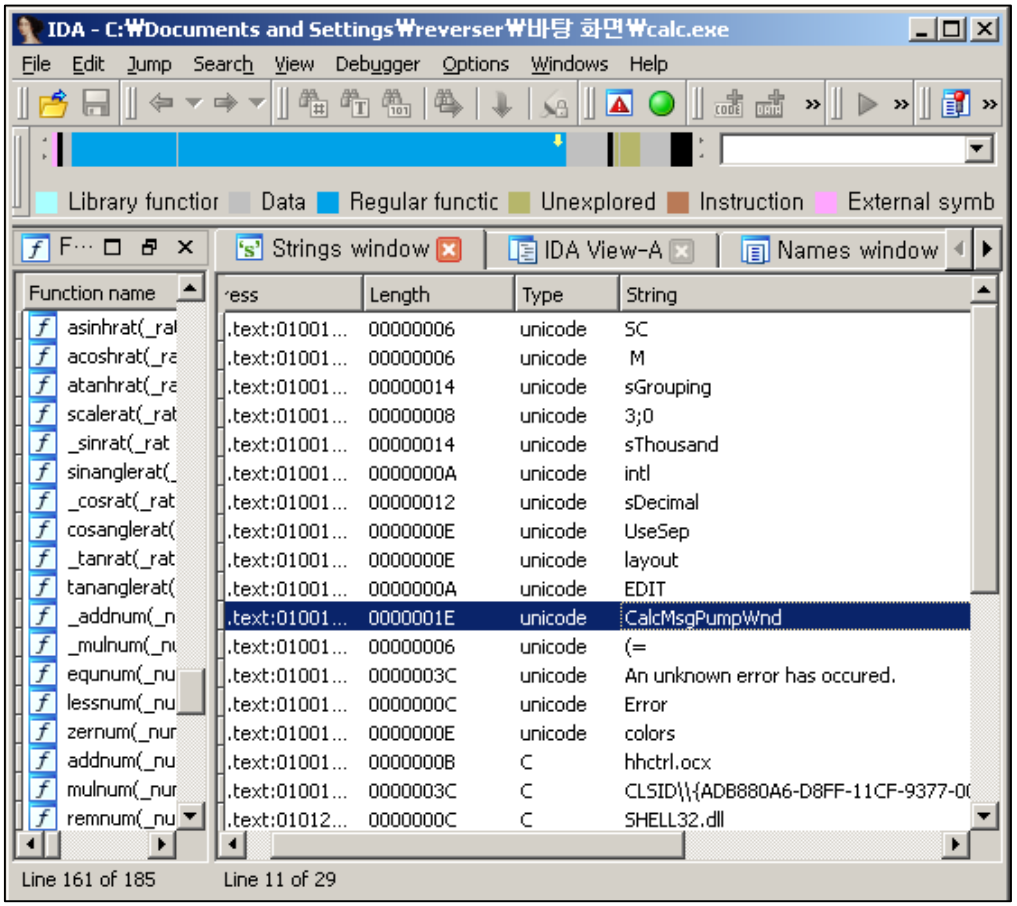
# IDA : Basic Usage

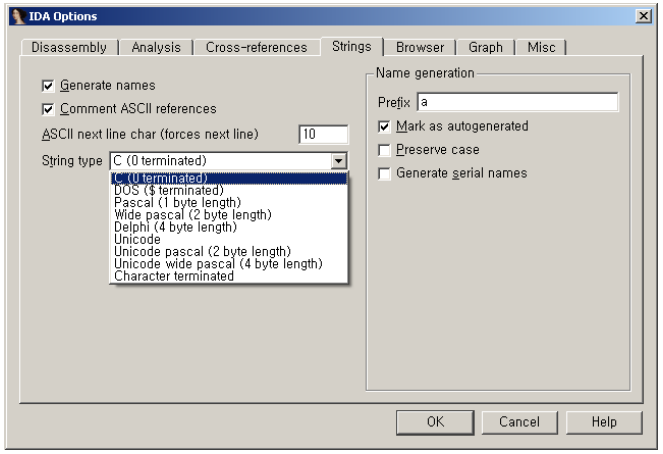
- **Names Window -'Shift + F4'**
  - Variables
  - Labels
  - Imported functions
  - Exported functions
  - ASCII strings
  - … …

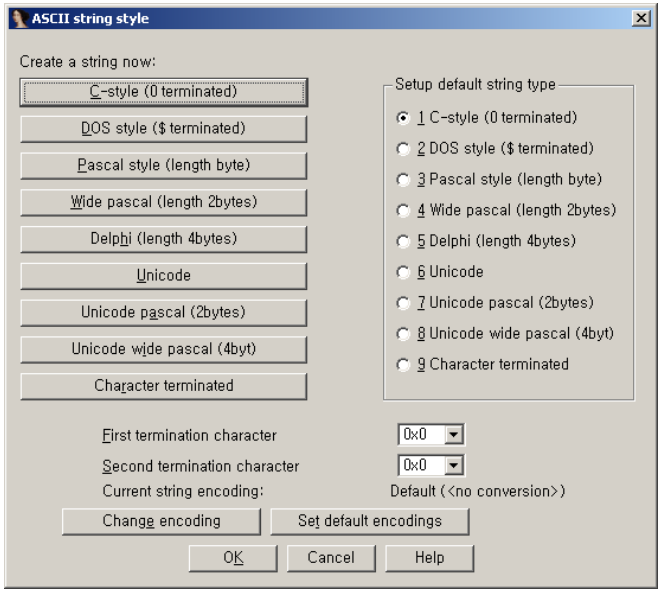


# IDA : Basic Usage

- **Strings Window -‘Shift + F12’**

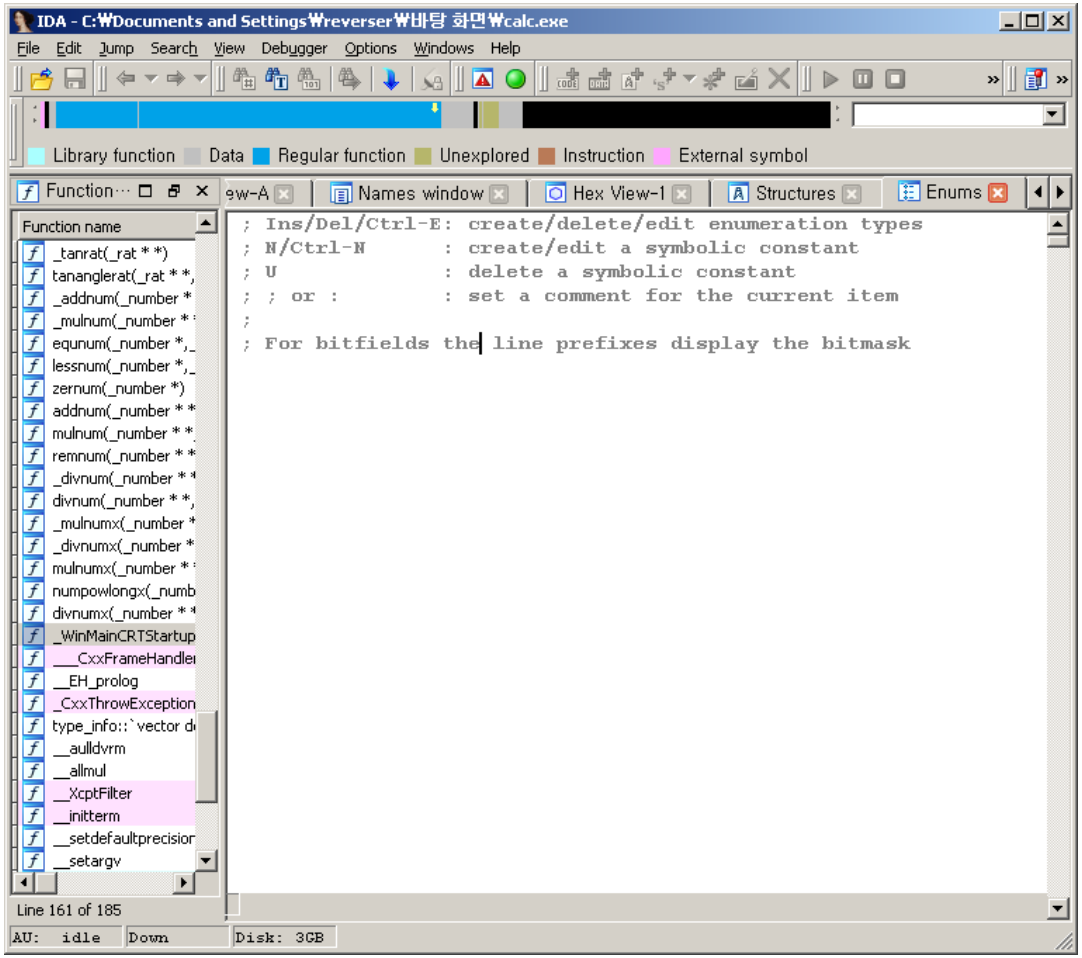


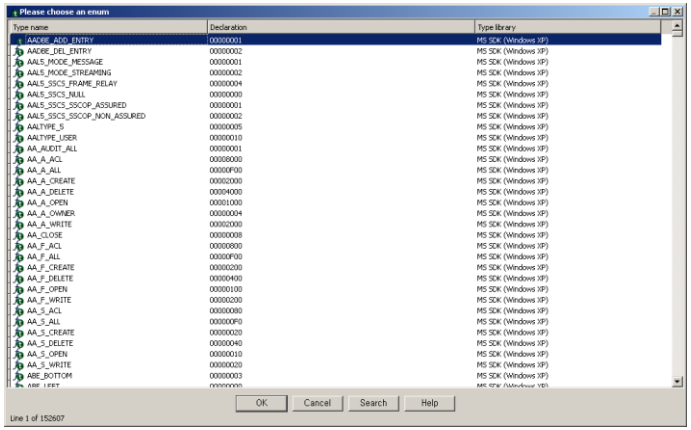



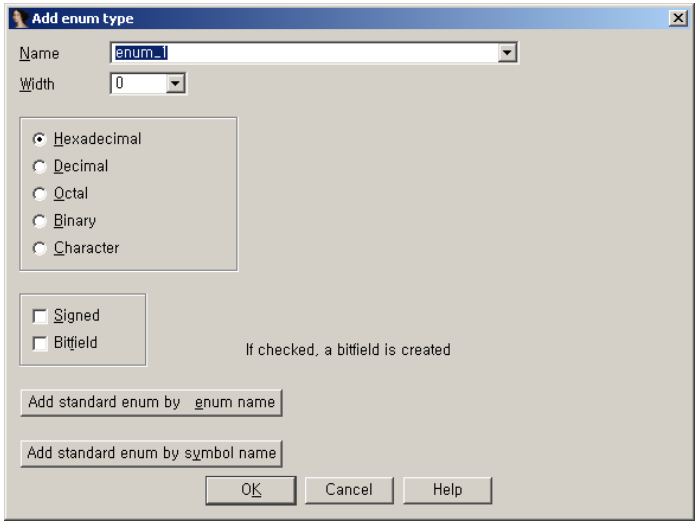



# IDA : Basic Usage

- **Enumerations Window -‘Shift + F10’**

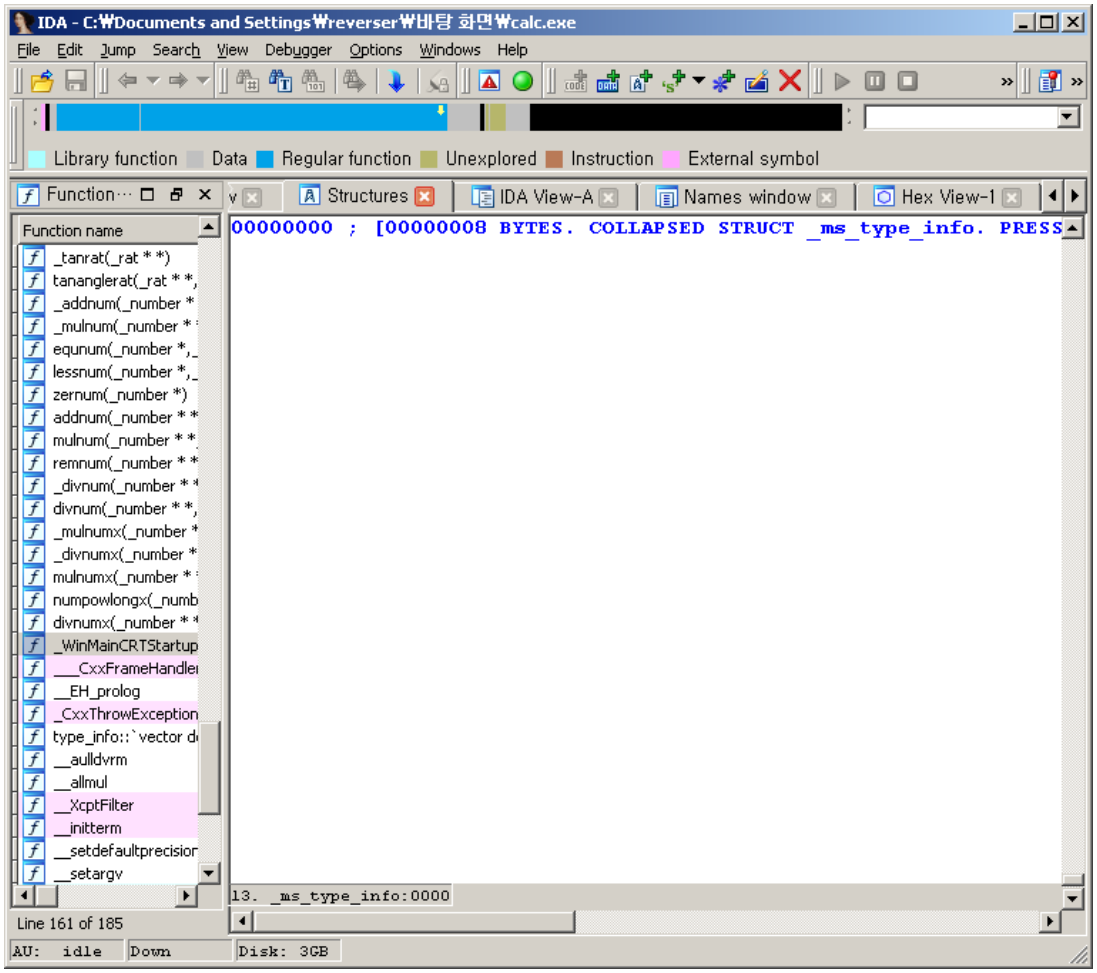


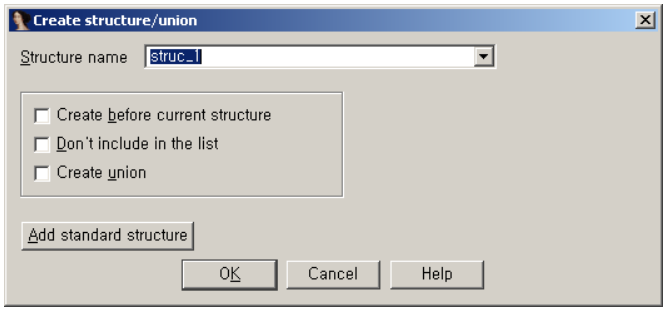



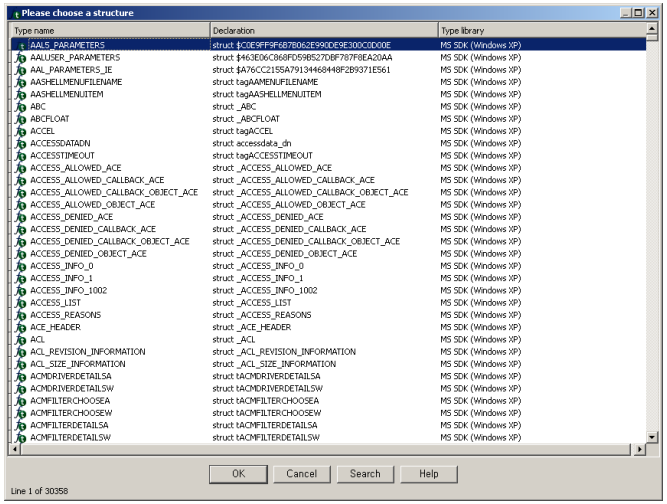



# IDA : Basic Usage

- **Structure Window -‘Shift + F9’**

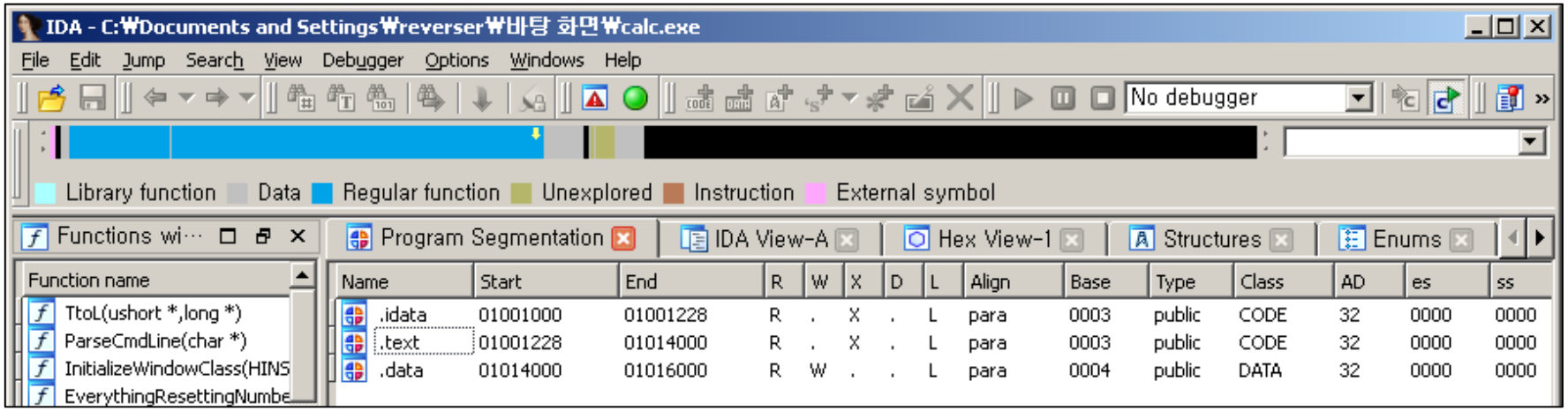


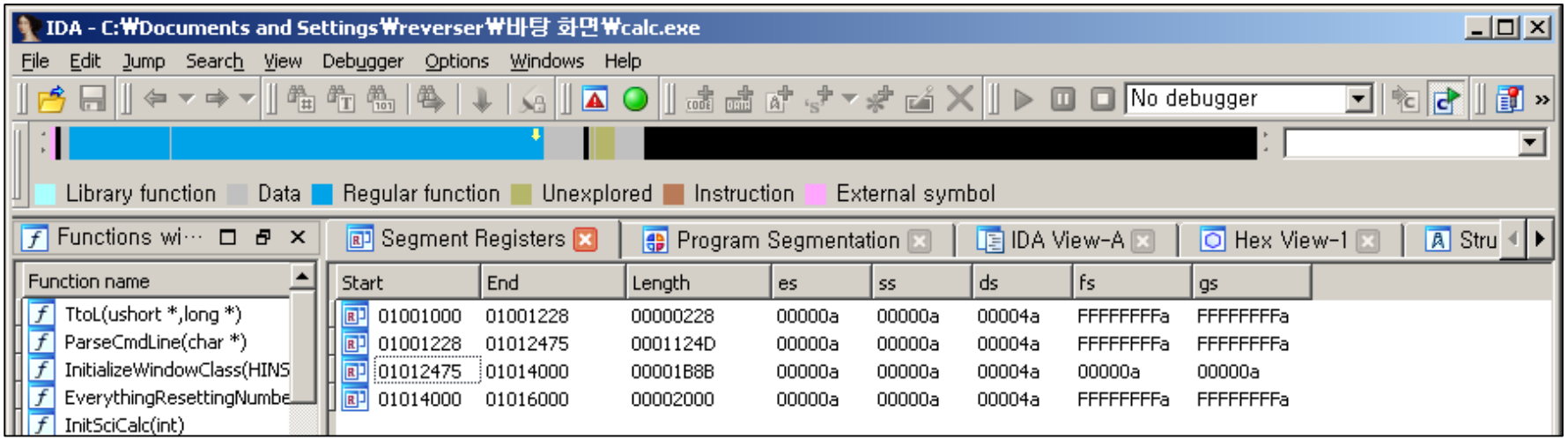



# IDA : Basic Usage

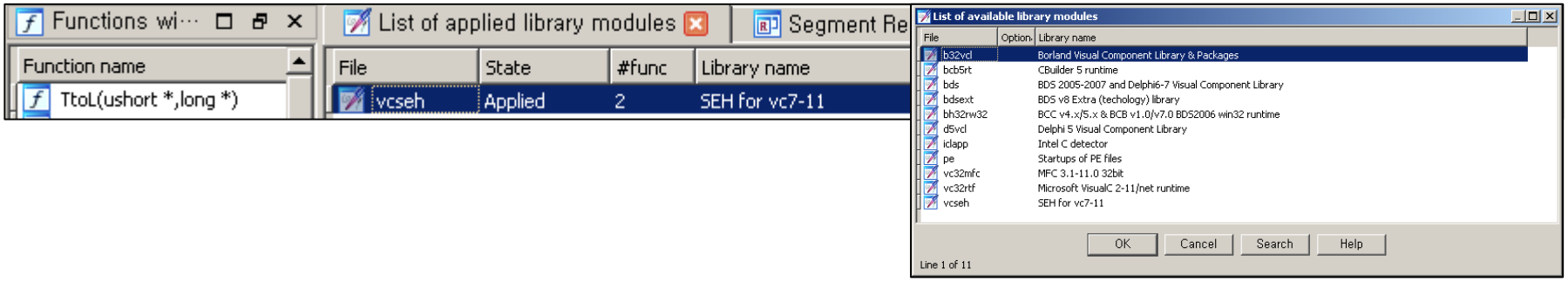
- **Segments / Segment Registers -‘Shift + F7’, ‘Shift + F8’**



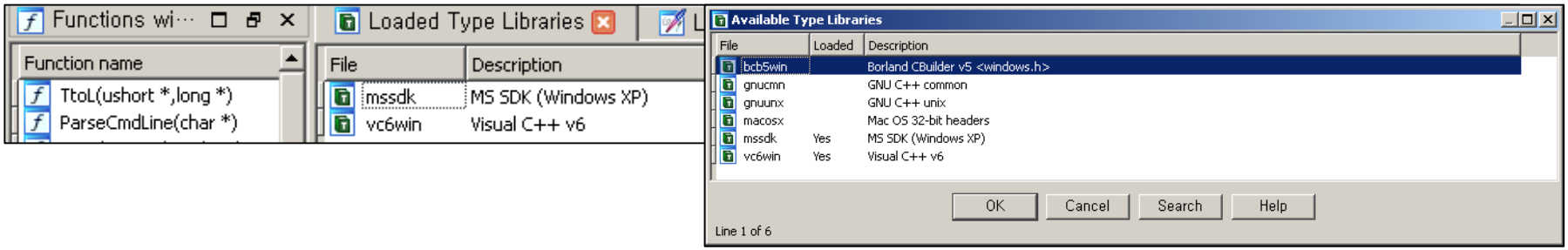



# IDA : Basic Usage

- **List of Applied Library Modules (%IDADIR%\sig) -‘Shift + F5’**




- **Loaded Type Libraries (%IDADIR%\til) -‘Shift + F11’**



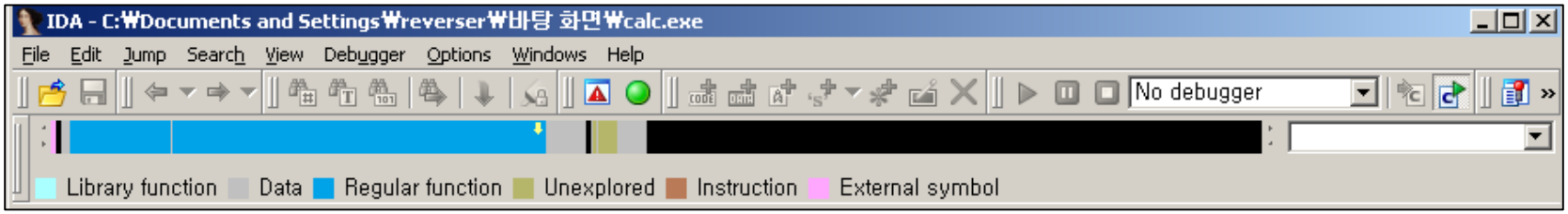
# IDA : Basic Usage

- **[Reference] Names Representation**
  - https://www.hex-rays.com/products/ida/support/idadoc/609.shtml

| Name Prefix | Description |
|---|---|
| sub_ | instruction, subroutine start (function) |
| locret_ | Address of 'return' instruction |
| loc_ | instruction address (label) |
| off_ | data, contains offset value |
| seg_ | data, contains segment address value |
| asc_ | data, ASCII string |
| byte_ | data, byte |
| word_ | data, 16-bits |
| dword_ | data, 32-bits |
| qword_ | data, 64-bits |
| xmmword_ | data, 128-bits |
| flt_ | floating point data, 32-bits |
| dbl_ | floating point data, 64-bits |
| tbyte_ | floating point data, 80-bits |
| stru_ | structure |
| custdata_ | custom data type |
| algn_ | alignment directive |
| unk_ | unexplored byte |

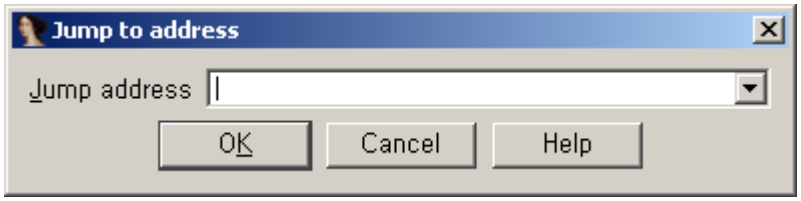
# IDA : Basic Usage

- **Navigator**



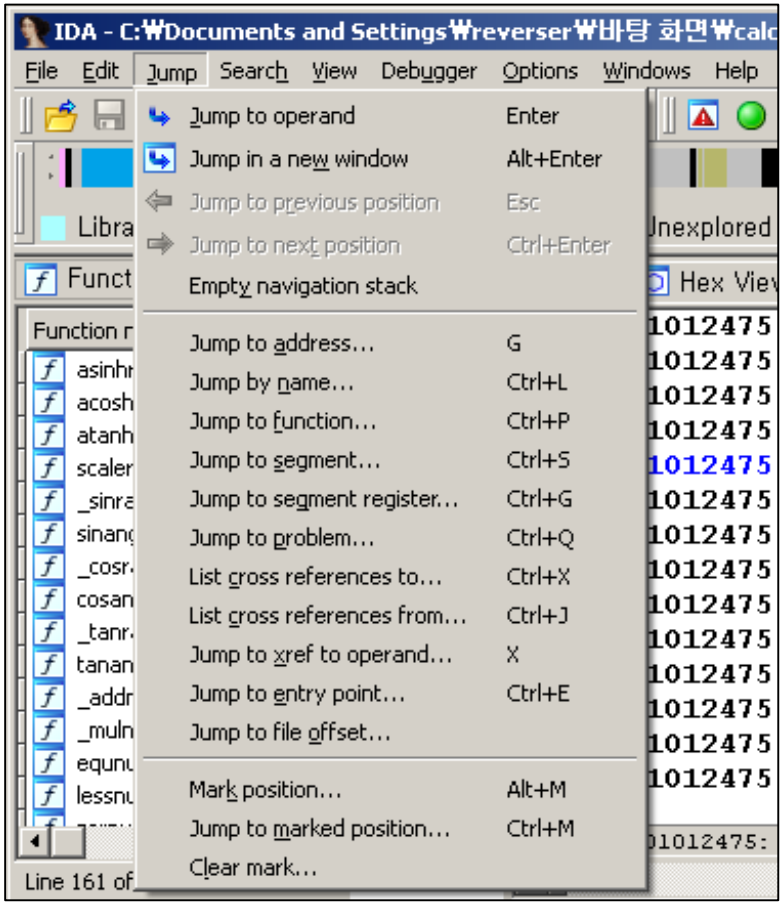

- **Click Navigation**
  - Previous -‘ESC’

- **Jump to Address**
  - Hotkey -‘g’



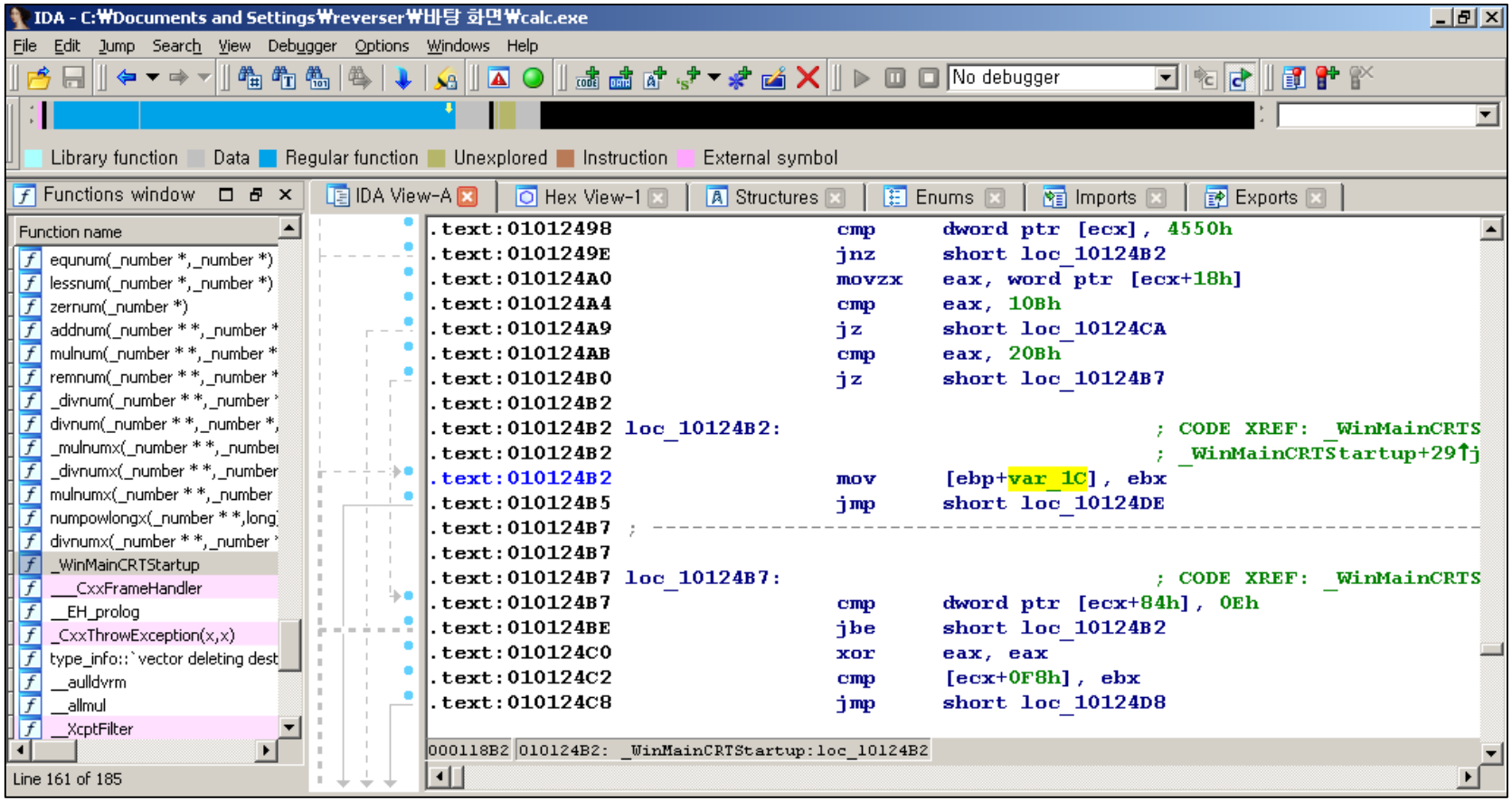
# IDA : Basic Usage

- **Jump operations**



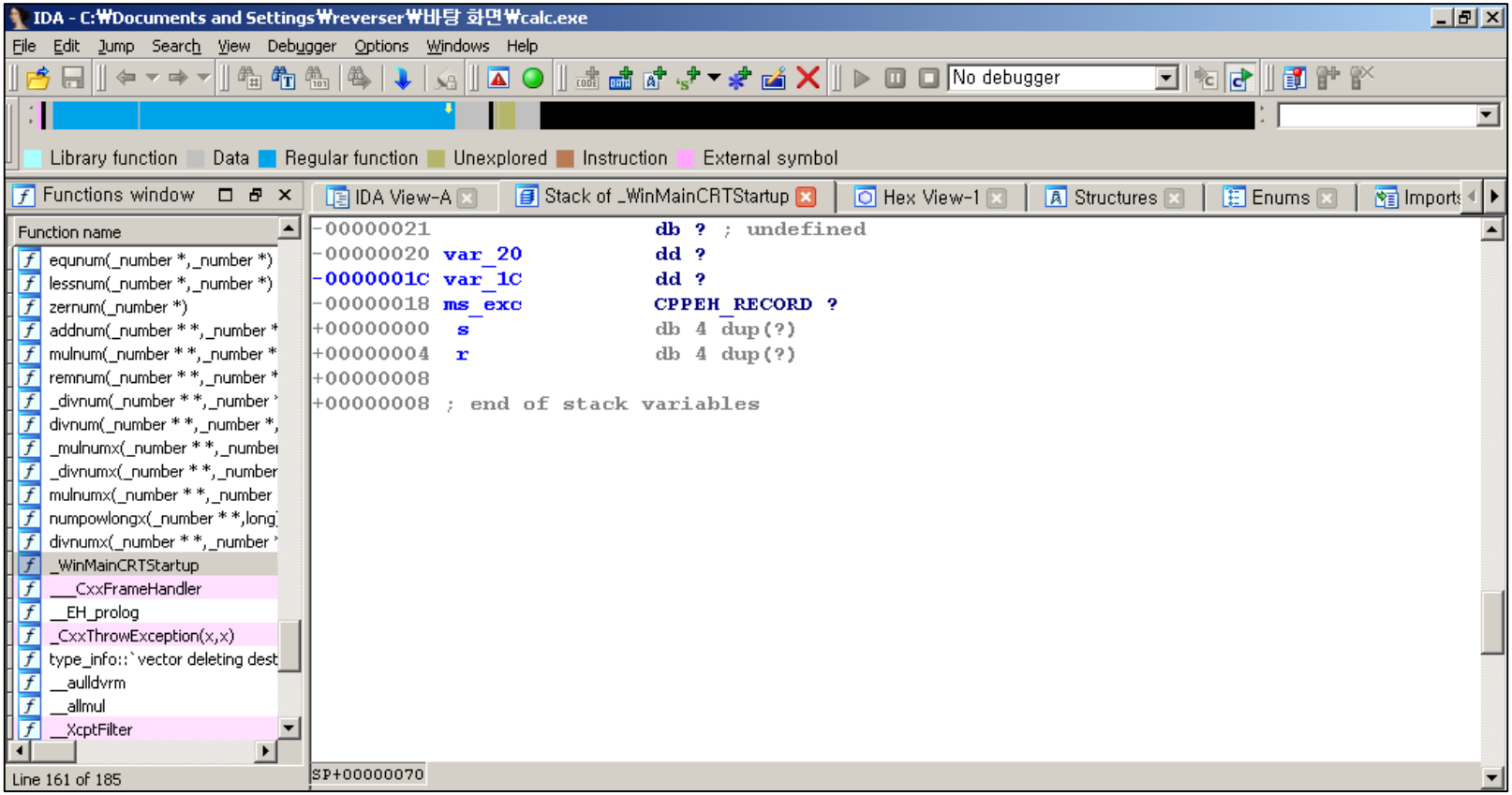
# IDA : Basic Usage

- **Stack Frames -‘Ctrl + K’**
  - Double click -‘var_*’ or ‘arg_*’



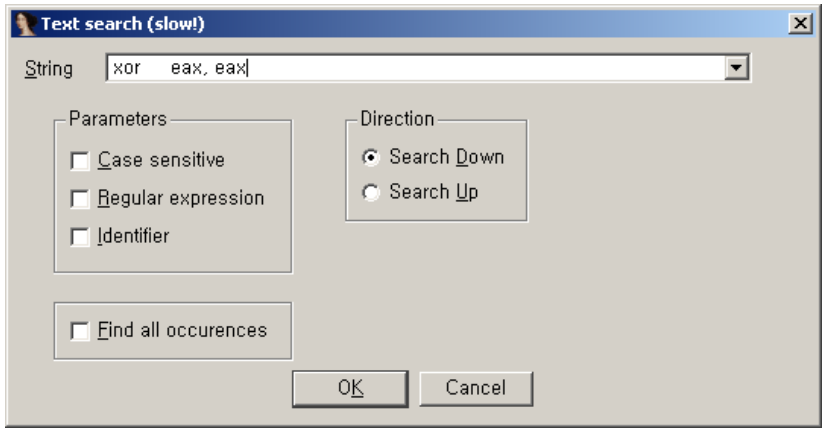
# IDA : Basic Usage

- **Stack Frames -‘Ctrl + K’**
  - Double click -‘var_*’ or ‘arg_*’

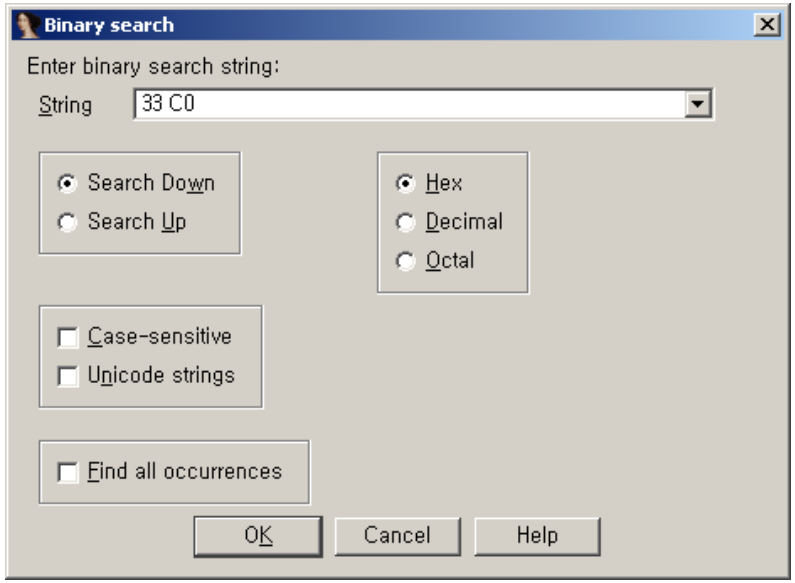


# IDA : Basic Usage

- **Searching Databases**
  - Text Search -‘Alt + T’

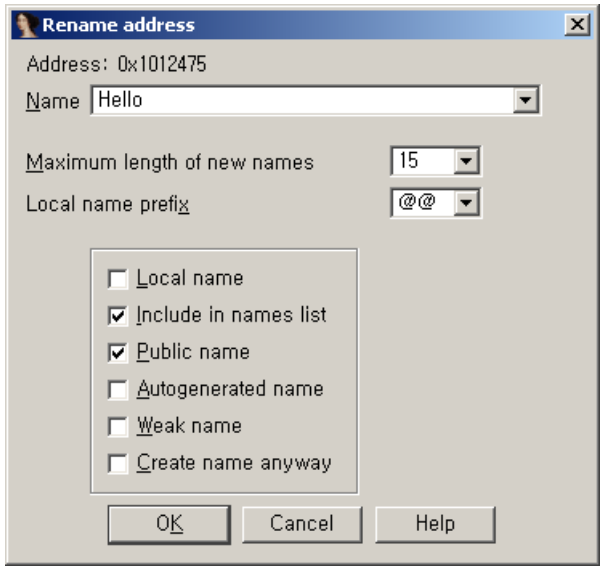


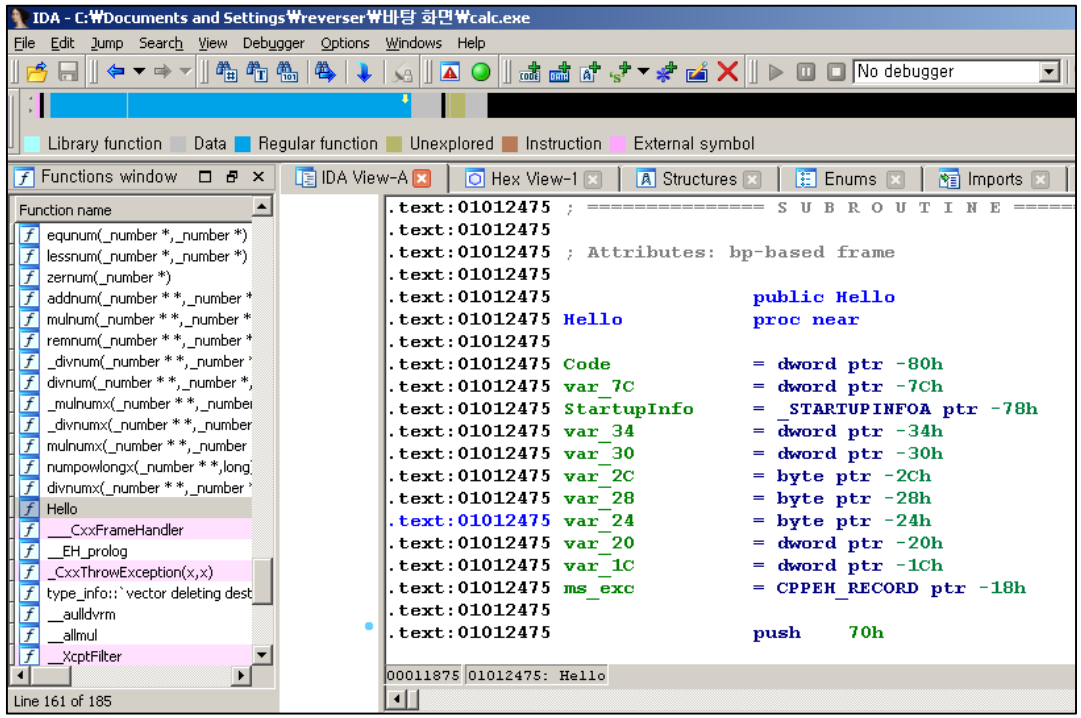

  - Binary Search -‘Alt + B’



# IDA : Basic Usage

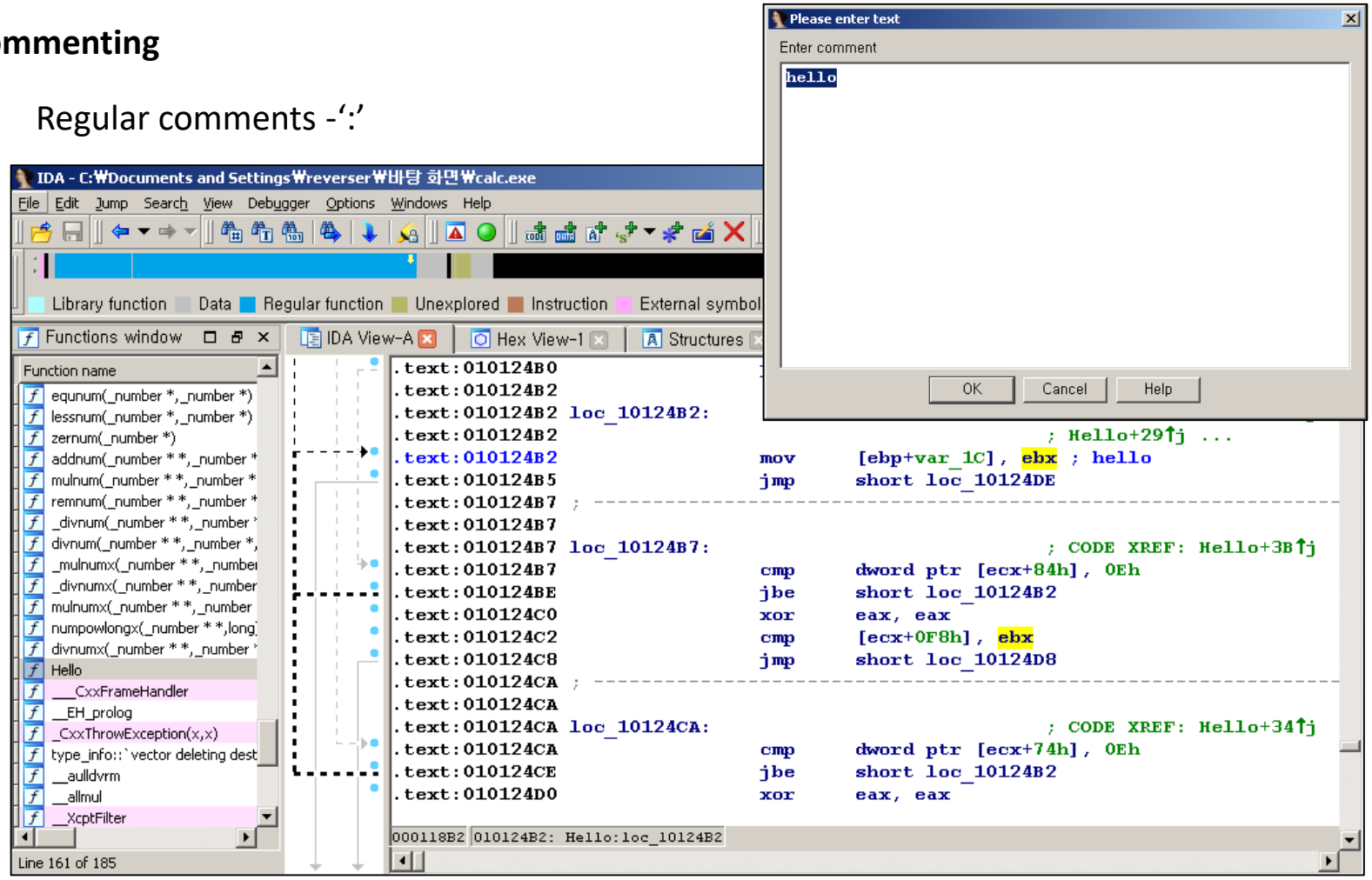
- **Names and Naming -‘N’**
  - Parameters and Local Variables
  - Named Location
  - Register Names



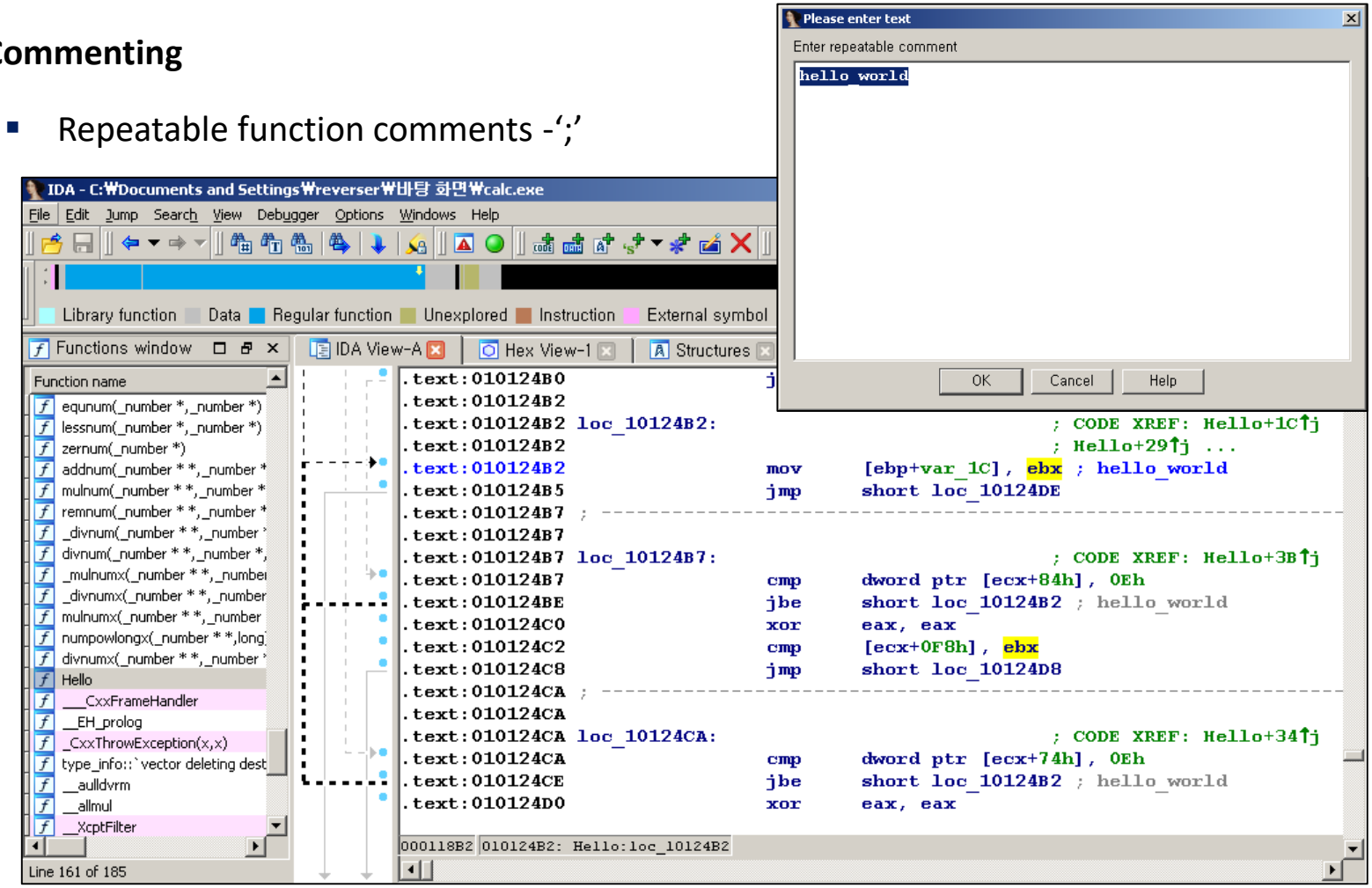
# IDA : Basic Usage

- **Commenting**
  - Regular comments -‘:’



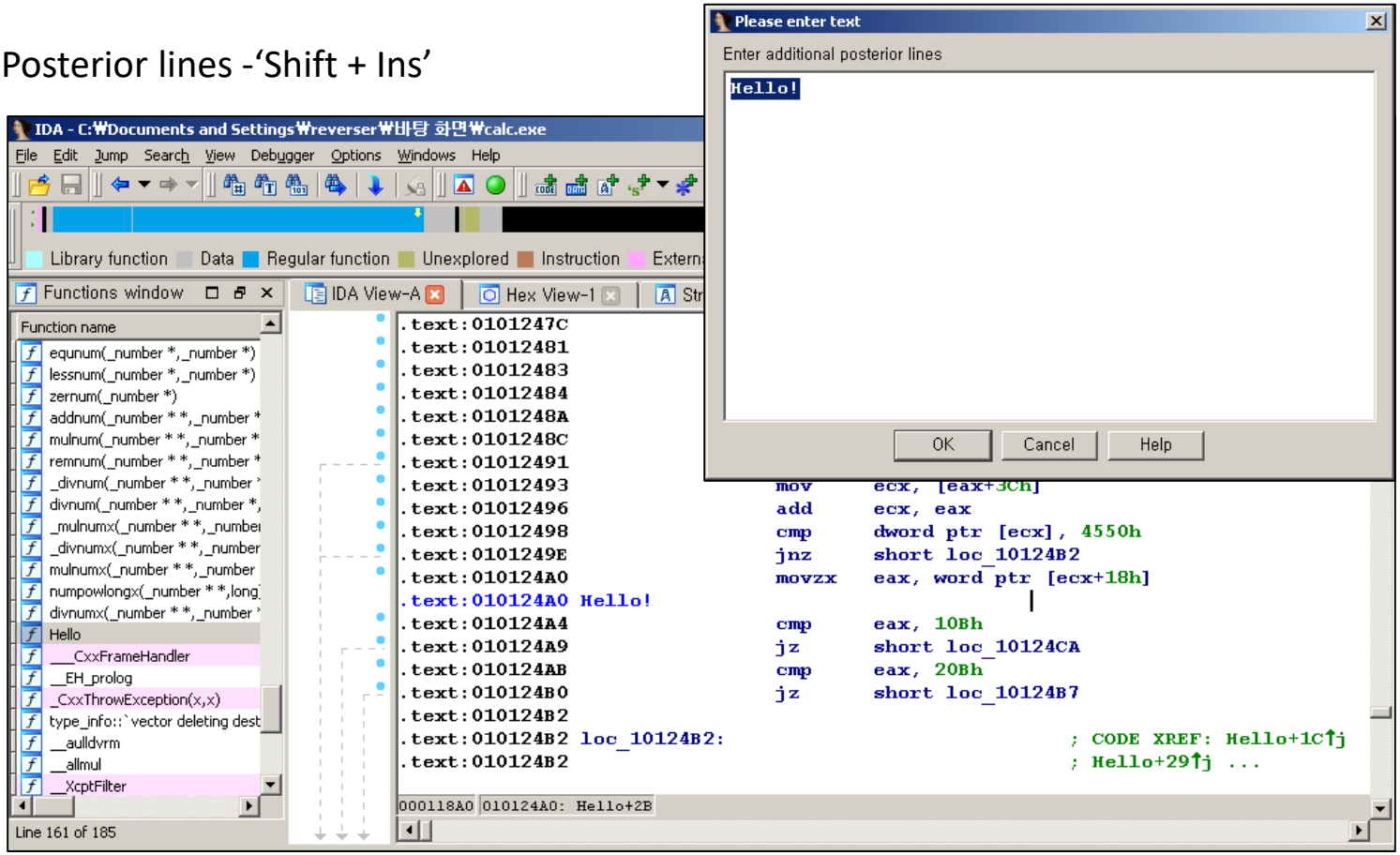
# IDA : Basic Usage

- **Commenting**
  - Repeatable function comments -‘;’



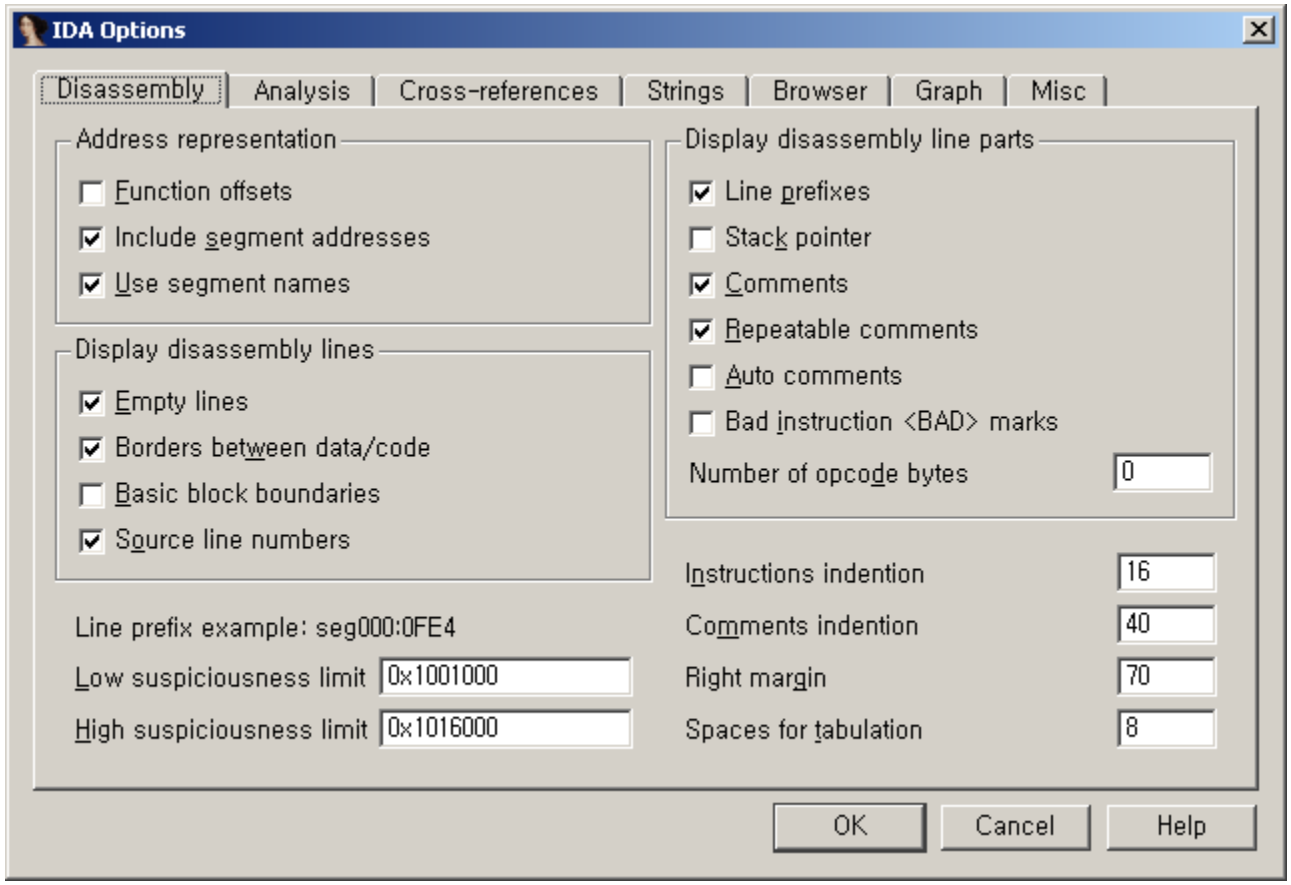
# IDA : Basic Usage

- **Commenting**
  - Anterior lines -‘Ins’
  - Posterior lines -‘Shift + Ins’



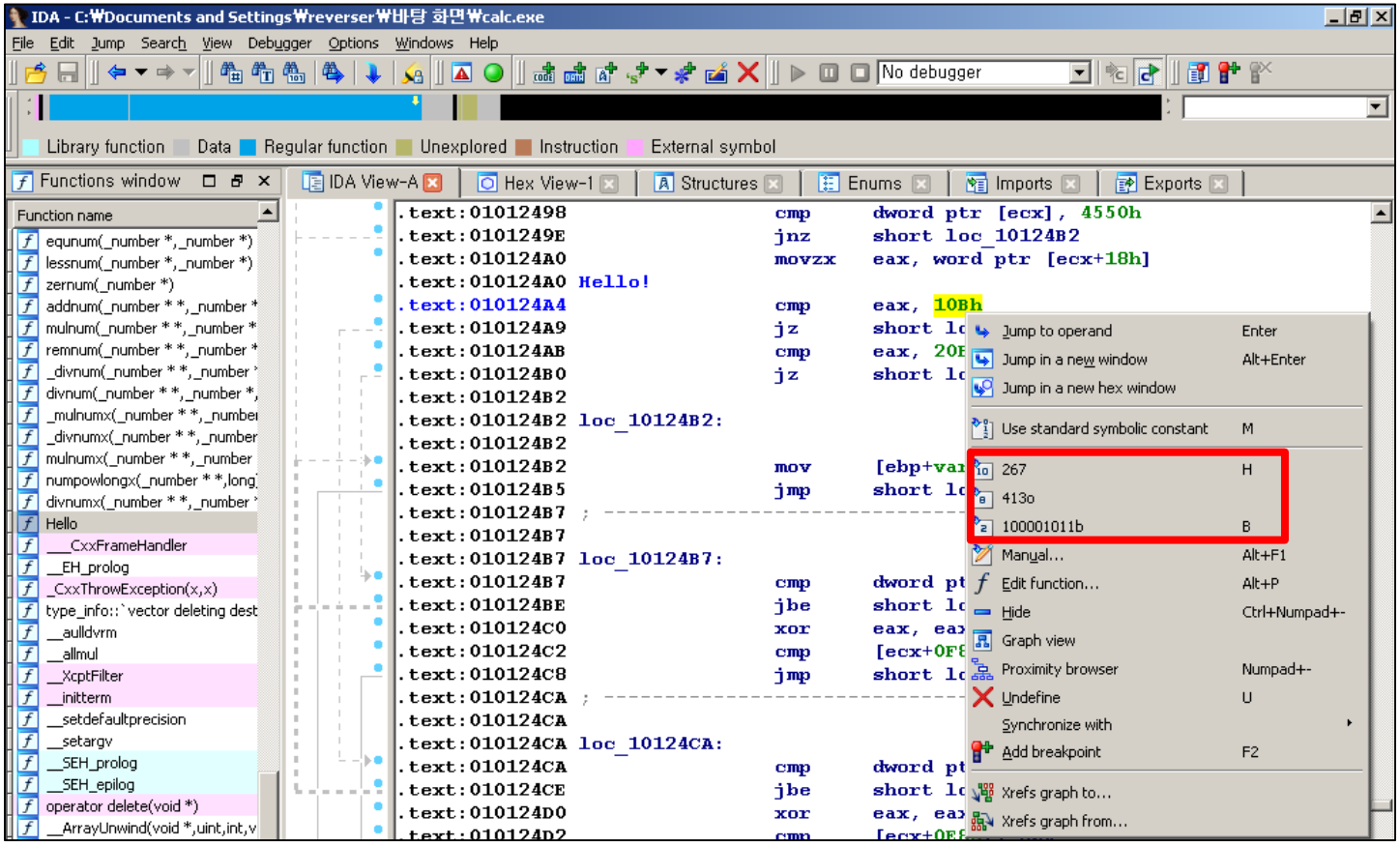
# IDA : Basic Usage

- **Code Transformations**
  - Disassembly line display options



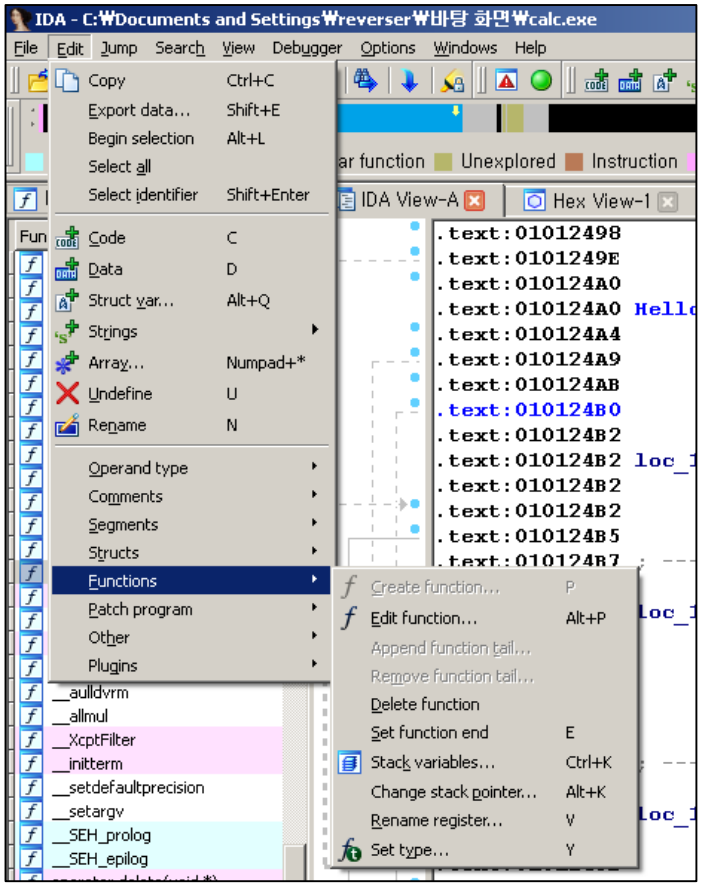
# IDA : Basic Usage

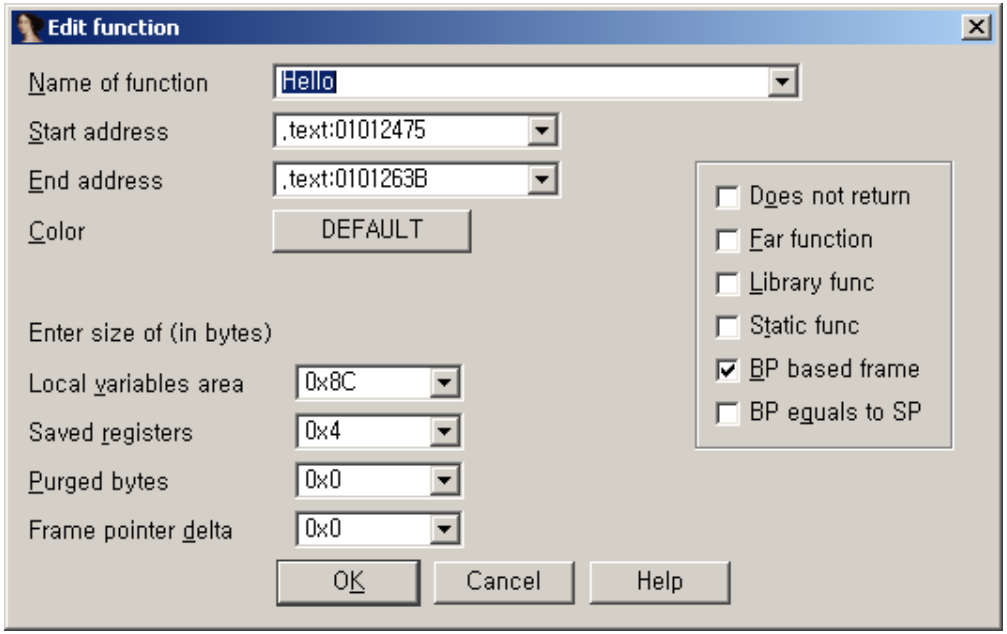
- **Code Transformations**
  - Formatting instruction operands



# IDA : Basic Usage

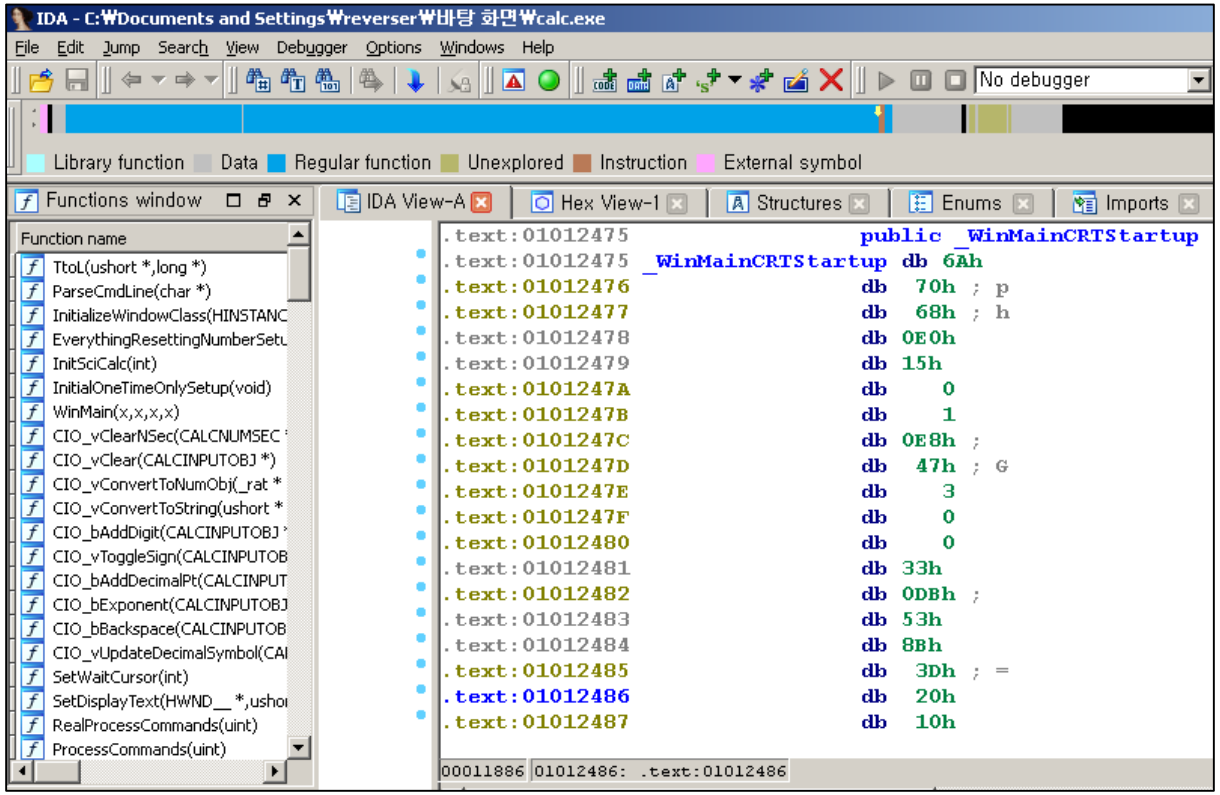
- **Code Transformations**
  - Manipulating functions



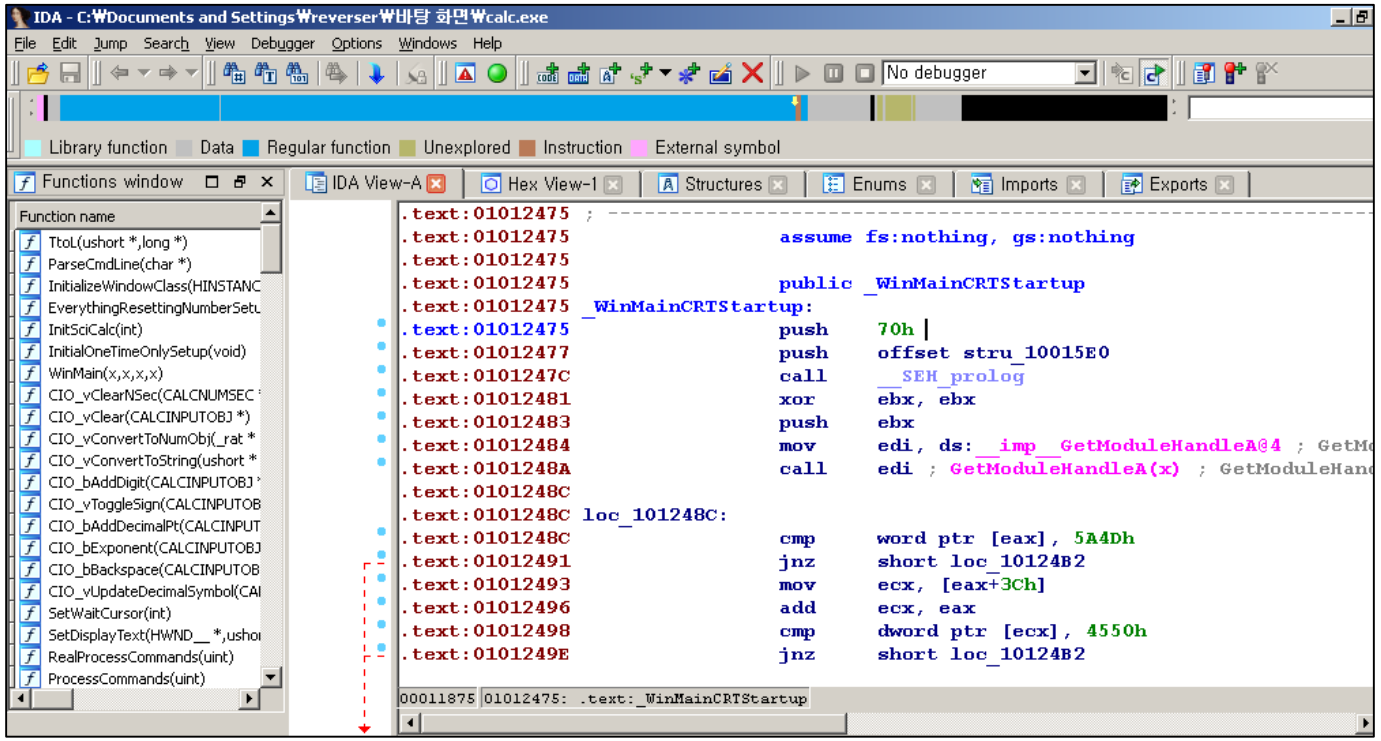
# IDA : Basic Usage

- **Code Transformations**
  - Converting code to data -‘D’
  - Converting data to code -‘C’

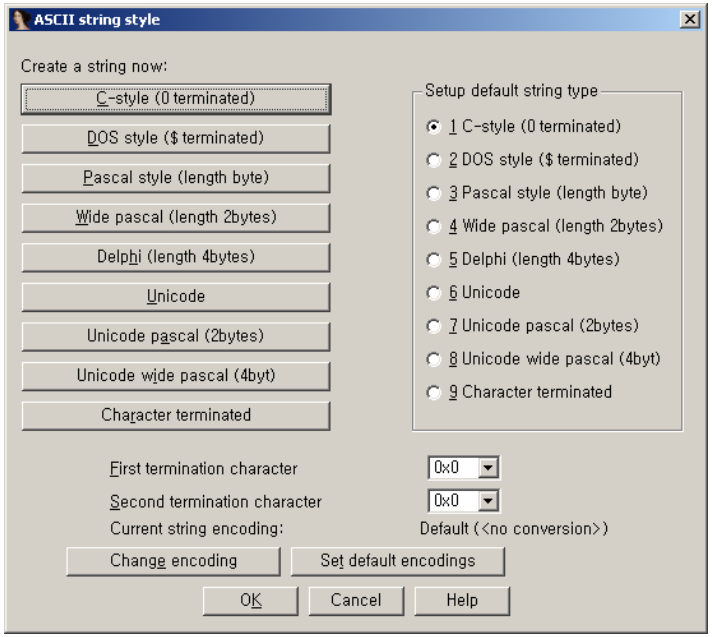
# IDA : Basic Usage

- **Code Transformations**
  - Converting code to data -‘D’
  - Converting data to code -‘C’

# IDA : Basic Usage

- **Data Transformations**
  - Working with Strings -‘Alt + A’
    - ASCII -‘A’

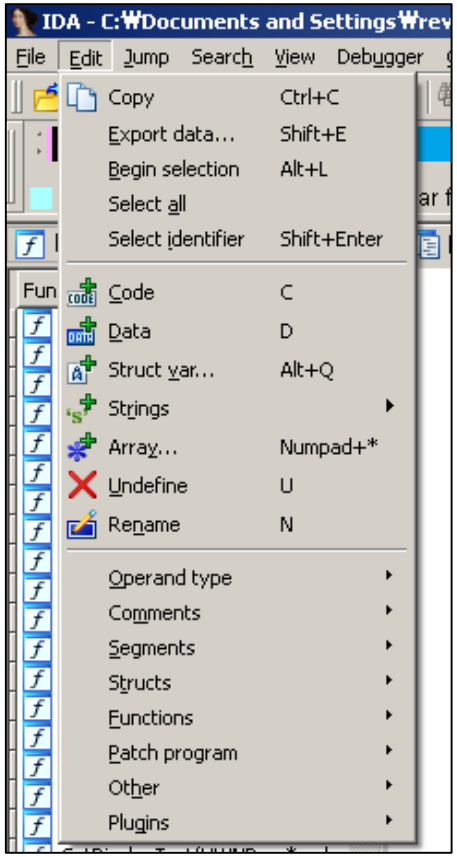



```
01001580 ; const WCHAR aColors
01001580 aColors:                                ; DATA XREF: CalcWndProc(HWND__
01001580                 unicode 0, <colors>,0
0100158E                 align 10h
01001590 ; CHAR byte_1001590[]
01001590 byte_1001590    db 68h                  ; DATA XREF: HtmlHelpW(x,x,x,x)
01001591                 db  68h ; h
01001592                 db  63h ; c
01001593                 db  74h ; t
01001594                 db  72h ; r
01001595                 db  6Ch ; l
01001596                 db  2Eh ; .
01001597                 db  6Fh ; o
01001598                 db  63h ; c
01001599                 db  78h ; x
0100159A                 db    0
0100159B                 align 10h
```

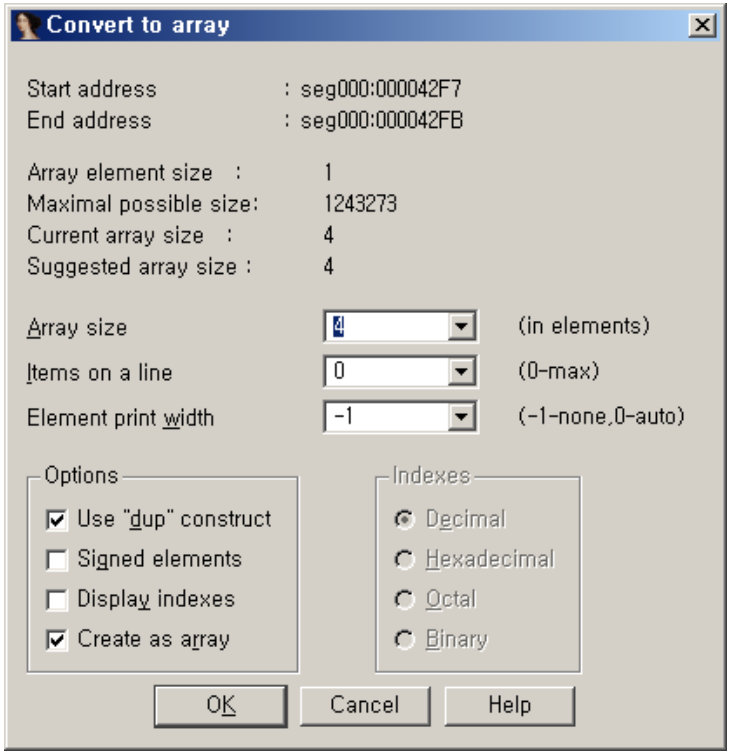
```
01001590 ; CHAR aHhctrl_ocx[]
01001590 aHhctrl_ocx     db 'hhctrl.ocx',0
0100159B                 align 10h
010015A0 ; CHAR SubKey[]
010015A0 SubKey          db 'CLSID\{ADB880A6-D8FF-
010015A0
010015DC ; CHAR ValueName[4]
010015DC ValueName       db 4 dup(0)
```

# IDA : Basic Usage

- **Data Transformations**
  - Specifying arrays -‘*’




```
00:000042F6                 db    1
00:000042F7                 db 95h, 0A2h, 0A8h, 0E5h
00:000042FB                 db 28h
00:000042FC                 db  6Ah ; j
00:000042FD                 db  5Fh ; _
00:000042FE                 db  8Fh ;
00:000042FF                 db 0BAh ;
00:00004300                 db 0EFh ;
```



# IDA : Basic Usage

- **Code Cross-References**

```
text:010124A4                   cmp     eax, 10Bh
text:010124A9                   jz      short loc_10124CA
text:010124AB                   cmp     eax, 20Bh
text:010124B0                   jz      short loc_10124B7
text:010124B2
text:010124B2 loc_10124B2:                              ; CODE XREF: _WinMainCRTStartup+1C↑j
text:010124B2                                           ; _WinMainCRTStartup+29↑j ...
text:010124B2                   mov     [ebp+hi], ebx
text:010124B5                   jmp     short loc_10124DE
text:010124B7 ; ---------------------------------------------------------------------------
text:010124B7
text:010124B7 loc_10124B7:                              ; CODE XREF: _WinMainCRTStartup+3B↑j
text:010124B7                   cmp     dword ptr [ecx+84h], 0Eh
text:010124BE                   jbe     short loc_10124B2
text:010124C0                   xor     eax, eax
text:010124C2                   cmp     [ecx+0F8h], ebx
text:010124C8                   jmp     short loc_10124D8
text:010124CA ; ---------------------------------------------------------------------------
text:010124CA
text:010124CA loc_10124CA:                              ; CODE XREF: _WinMainCRTStartup+34↑j
text:010124CA                   cmp     dword ptr [ecx+74h], 0Eh
text:010124CE                   jbe     short loc_10124B2
text:010124D0                   xor     eax, eax
text:010124D2                   cmp     [ecx+0E8h], ebx
text:010124D8
text:010124D8 loc_10124D8:                              ; CODE XREF: _WinMainCRTStartup+53↑j
text:010124D8                   setnz   al
text:010124DB                   mov     [ebp+hi], eax
text:010124DE
text:010124DE loc_10124DE:                              ; CODE XREF: _WinMainCRTStartup+40↑j
text:010124DE                   mov     [ebp+ms_exc.registration.TryLevel], ebx
text:010124E1                   push    2
text:010124E3                   call    ds:__imp____set_app_type
```

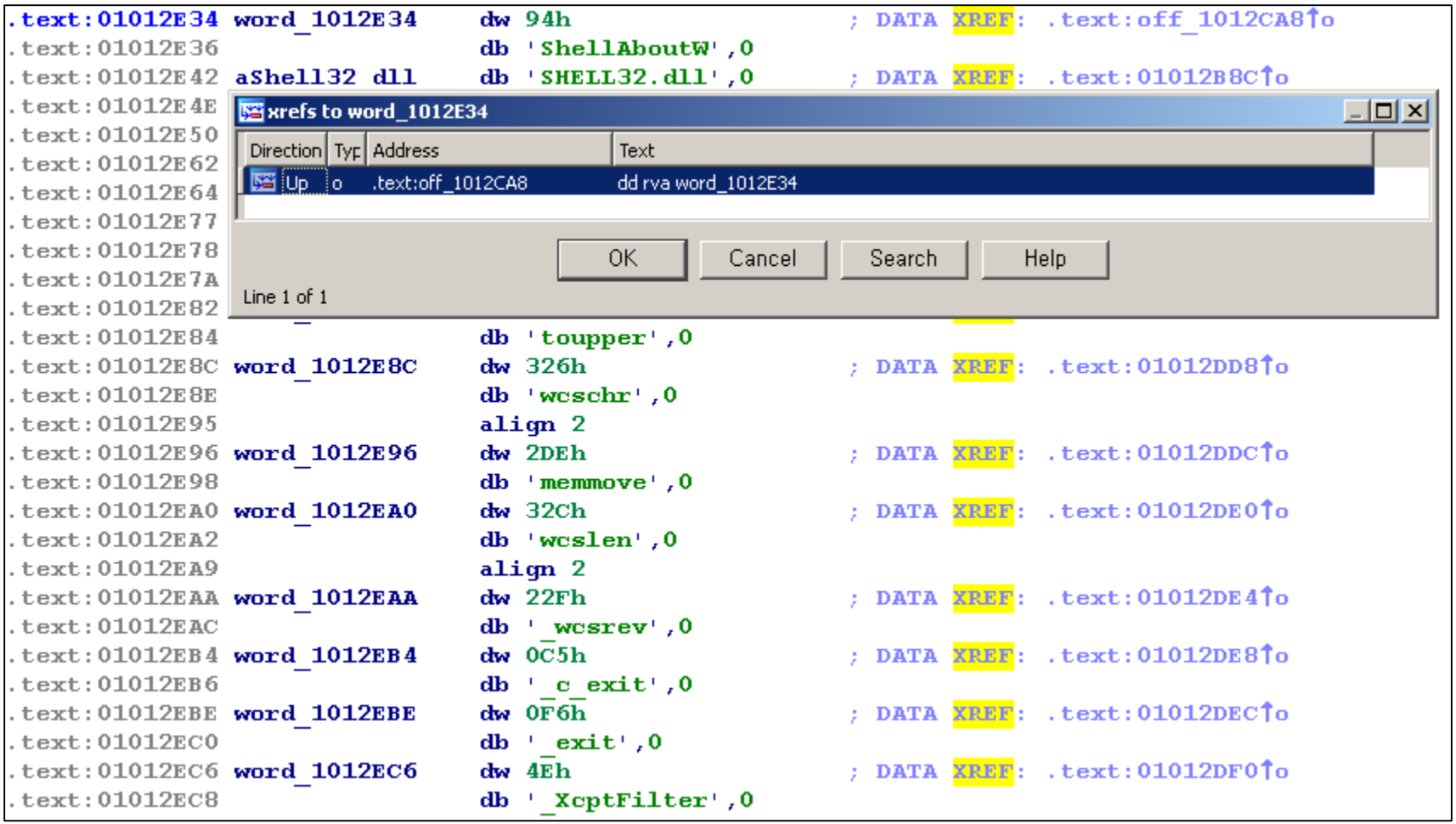
# IDA : Basic Usage

- **Data Cross-References**

```
text:01012E34 word_1012E34     dw 94h                  ; DATA XREF: .text:off_1012CA8
text:01012E36                  db 'ShellAboutW',0
text:01012E42 aShell32_dll     db 'SHELL32.dll',0      ; DATA XREF: .text:01012B8C↑o
text:01012E4E word_1012E4E     dw 52h                  ; DATA XREF: .text:off_1012DC8
text:01012E50                  db '__CxxFrameHandler',0
text:01012E62 word_1012E62     dw 47h                  ; DATA XREF: .text:01012DCC↑o
text:01012E64                  db '_CxxThrowException',0
text:01012E77                  align 4
text:01012E78 word_1012E78     dw 338h                 ; DATA XREF: .text:01012DD0↑o
text:01012E7A                  db 'wcstoul',0
text:01012E82 word_1012E82     dw 31Ah                 ; DATA XREF: .text:01012DD4↑o
text:01012E84                  db 'toupper',0
text:01012E8C word_1012E8C     dw 326h                 ; DATA XREF: .text:01012DD8↑o
text:01012E8E                  db 'wcschr',0
text:01012E95                  align 2
text:01012E96 word_1012E96     dw 2DEh                 ; DATA XREF: .text:01012DDC↑o
text:01012E98                  db 'memmove',0
text:01012EA0 word_1012EA0     dw 32Ch                 ; DATA XREF: .text:01012DE0↑o
text:01012EA2                  db 'wcslen',0
text:01012EA9                  align 2
text:01012EAA word_1012EAA     dw 22Fh                 ; DATA XREF: .text:01012DE4↑o
text:01012EAC                  db '_wcsrev',0
text:01012EB4 word_1012EB4     dw 0C5h                 ; DATA XREF: .text:01012DE8↑o
text:01012EB6                  db '_c_exit',0
text:01012EBE word_1012EBE     dw 0F6h                 ; DATA XREF: .text:01012DEC↑o
text:01012EC0                  db '_exit',0
text:01012EC6 word_1012EC6     dw 4Eh                  ; DATA XREF: .text:01012DF0↑o
text:01012EC8                  db '_XcptFilter',0
text:01012ED4 word_1012ED4     dw 0C8h                 ; DATA XREF: .text:01012DF4↑o
text:01012ED6                  db '_cexit',0
text:01012EDD                  align 2
```

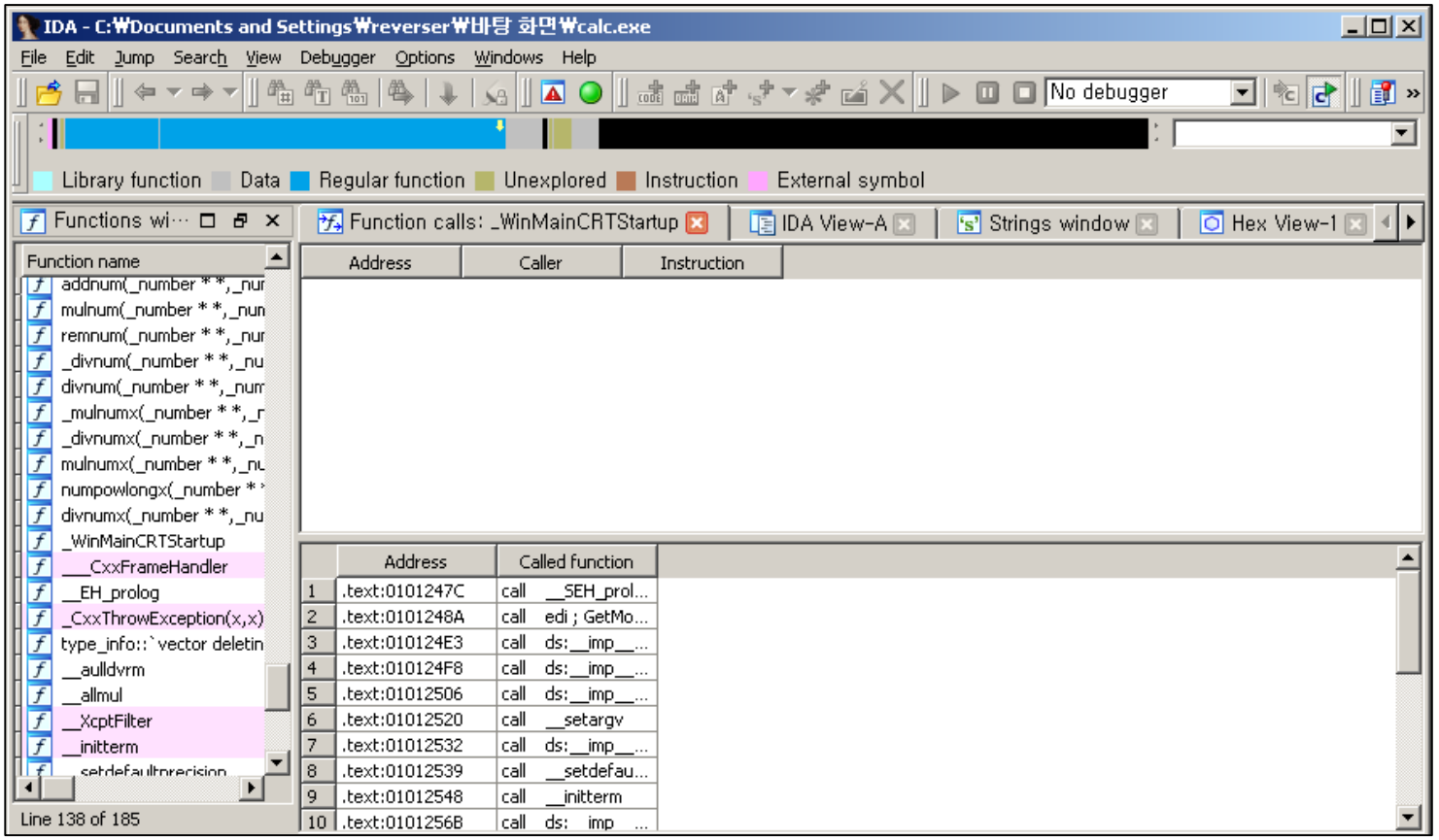
# IDA : Basic Usage

- **Cross-References Lists -‘Ctrl + X’**



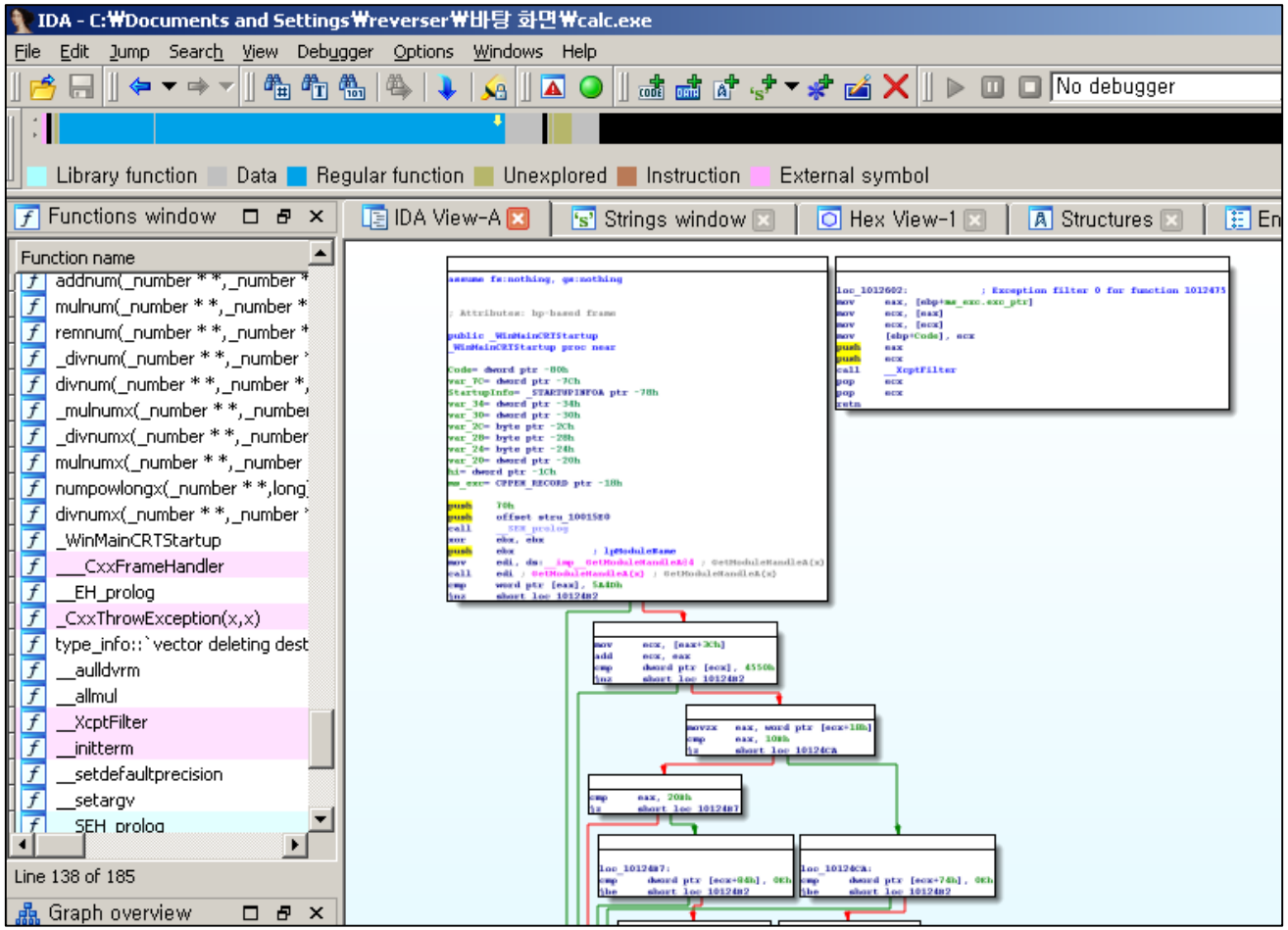
# IDA : Basic Usage

- **Function Calls**
  - View -Open subviews-Function calls



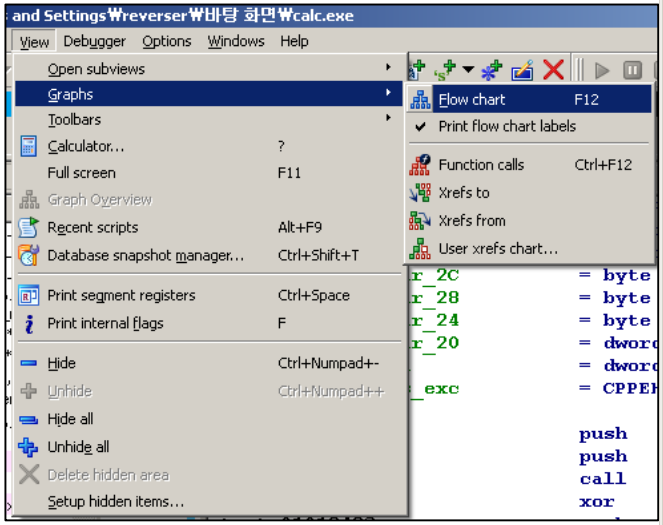
# IDA : Basic Usage

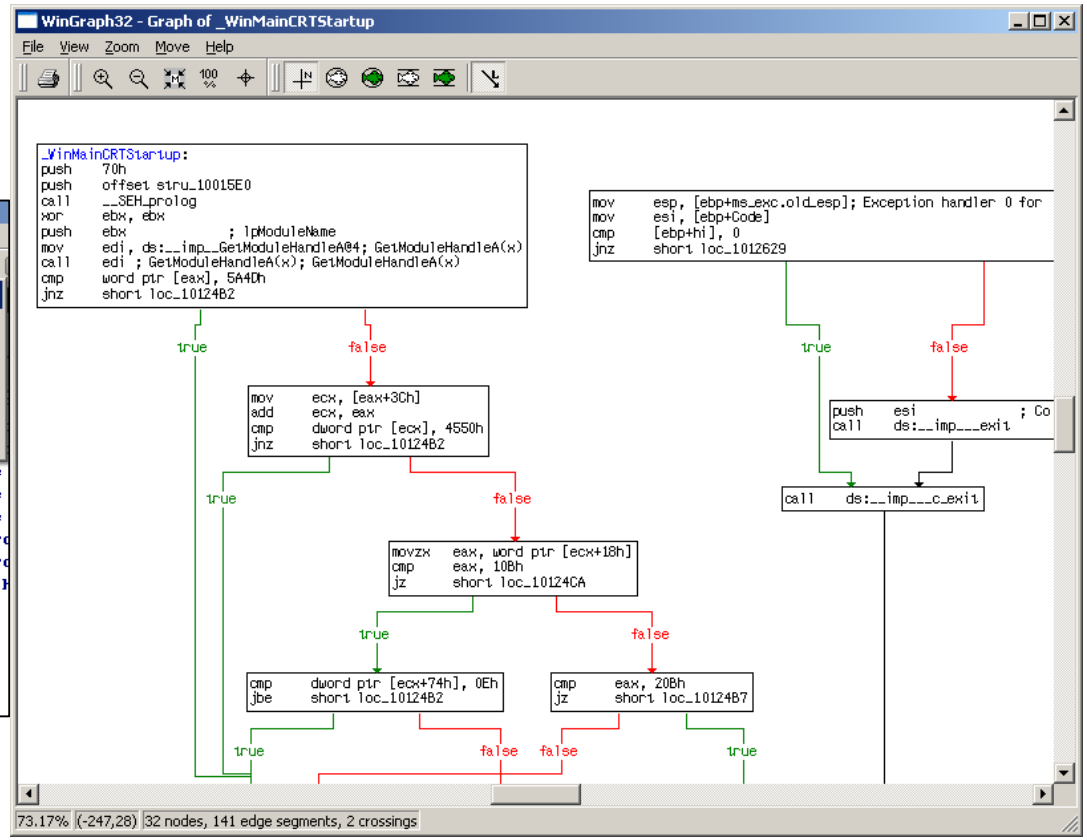
- **Integrated Graph View**



# IDA : Basic Usage

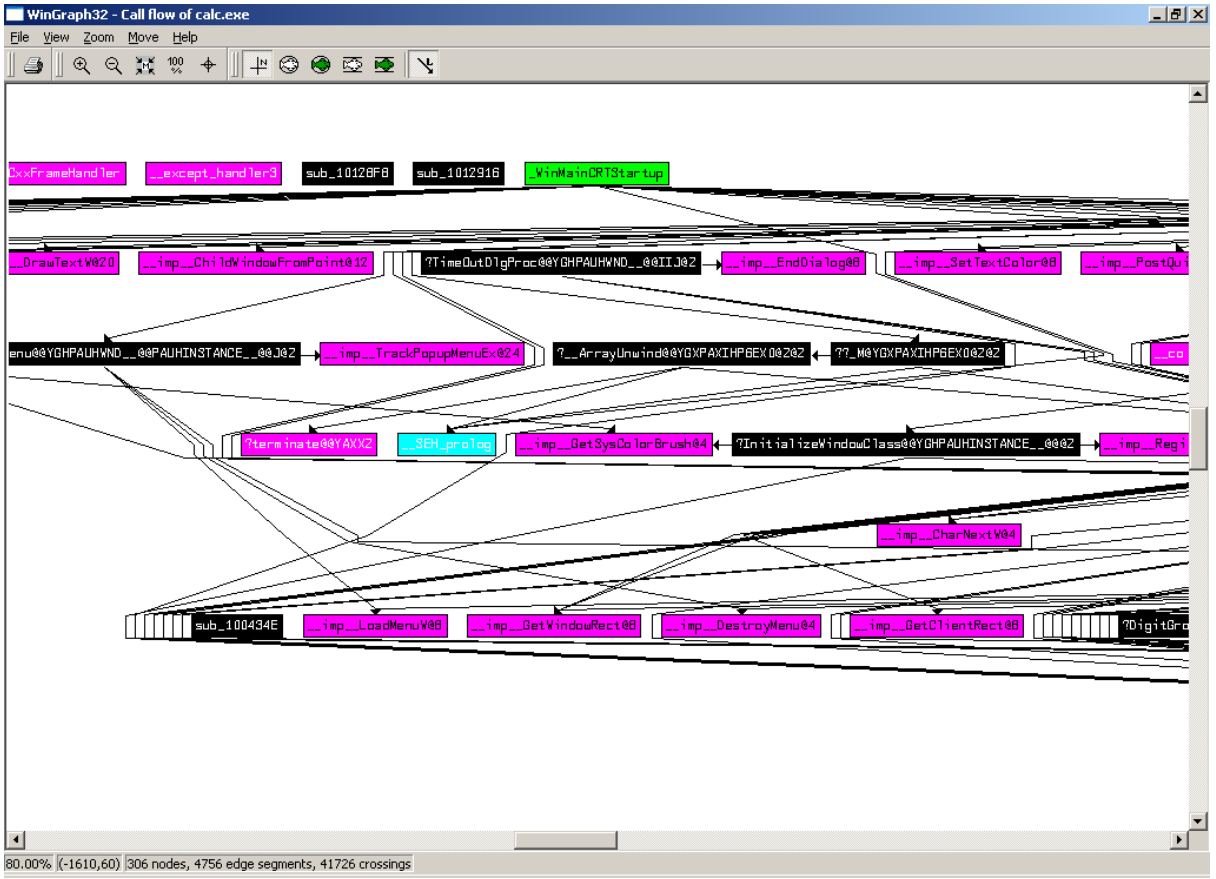
- **External Graphing**
  - Flow chart -‘F12’



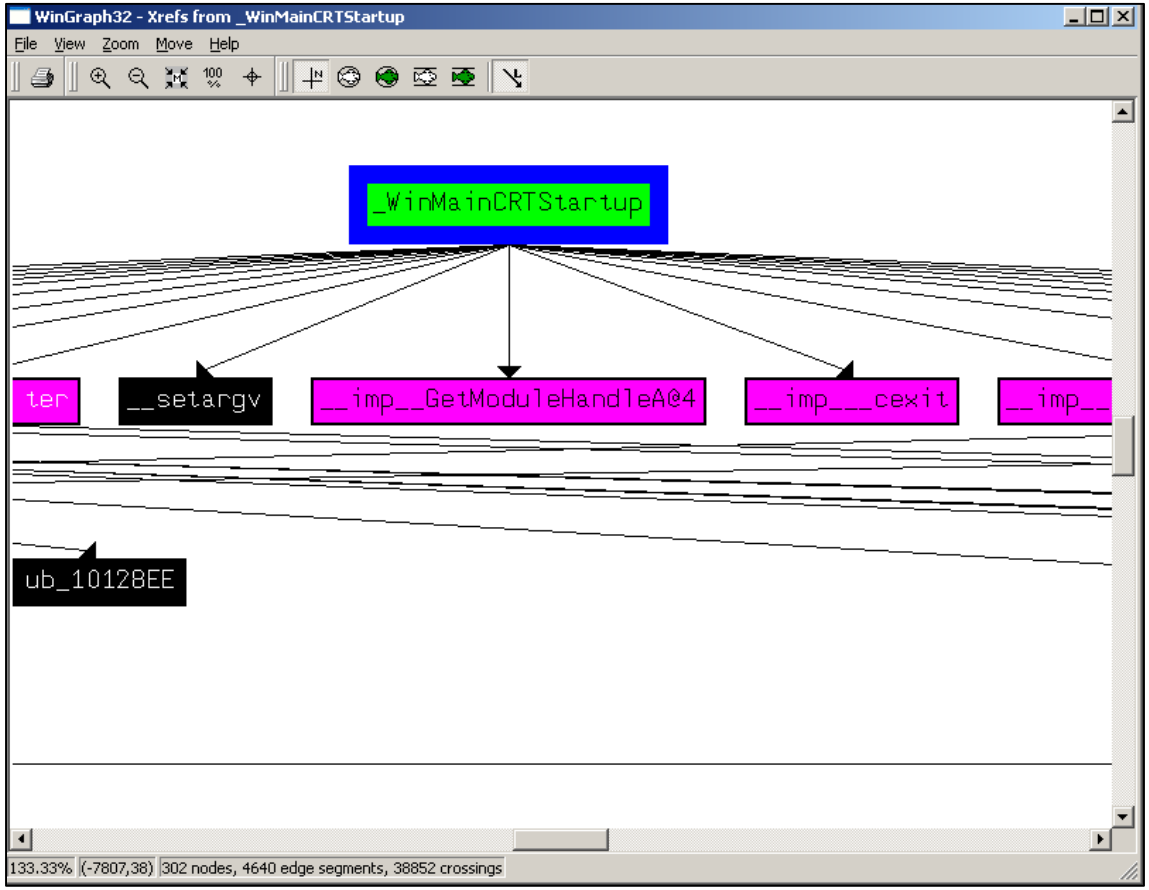
# IDA : Basic Usage

- **External Graphing**
  - Function calls -‘Ctrl + F12’



# IDA : Basic Usage

- **External Graphing**
  - Xrefsgraph to / from



# Thank you for listening


koha@korea.ac.kr