逆向工程基礎入門實務

TDOH-workshop
Leg_Bone

首先……

這是個很輕鬆的
演(聊)講(天)

在跟大家聊天的過程中
大家只要.....

聽台上那個人

<del> 唬爛 </del>

把該記的好好記住

最好是跟著做!
這是workshop!!!!

 把不該記的全忘掉

貼心提醒

在聊天的過程中.....

有什麼問題隨時舉手提問

可以睡覺

但是打呼不要吵到人

聊天不要比我大聲

請不要拿垃圾丟我！！！！

<(_ _)> m(_ _)m <(_ _)>

P.S 這次會有很多很多很多的**Live demo**
所以如果不幸凸槌請不要揍我**QQ**

<(_ _)> m(_ _)m <(_ _)>

大家好~ 我是腿骨

About Me

撰寫BY PASS Hackshield

TDOHacker 南區召集人

SITCON 2014/2015 short talk 講者

About Me

晶睿科技資安實習生

~~穩定單身中的小小魯蛇Q_Q~~

然後我的實際身分.....

是個廚師

聽完下面這場workshop,你可以.....

還是只能逆一些簡單的小東西T_T

每個DEMO都會留時間給各位練習實做

在開始前我想了解一下各位同學對逆向工程的認知

逆向工程（又稱反向工程），是一種技術過程，即對一專案標產品進行逆向分析及研究，從而演繹並得出該產品的處理流程、組織結構、功能效能規格等設計要素，以製作出功能相近，但又不完全一樣的產品。逆向工程源於商業及軍事領域中的硬體分析。其主要目的是，在不能輕易獲得必要的生產資訊下，直接從成品的分析，推匯出產品的設計原理。

逆向工程可能會被誤認為是對智慧財產權的嚴重侵害，但是在實際應用上，反而可能會保護智慧財產權所有者。例如在積體電路領域，如果懷疑某公司侵犯智慧財產權，可以用逆向工程技術來尋找證據。

這邊有誰學過C/C++?哪種C/C++?

那這邊有誰學過**ASM(**assembly language**)**
又是哪種ASM??

前置技能:會寫CODE,看得懂ASM

本日課程

逆向基礎詳解

1.OLLYDBG實作演練

Crack me破解

商業軟體010Editor破解

2.IDA實作演練

Crack me破解

商業軟體010Editor破解

3.Cheat engine實作演練

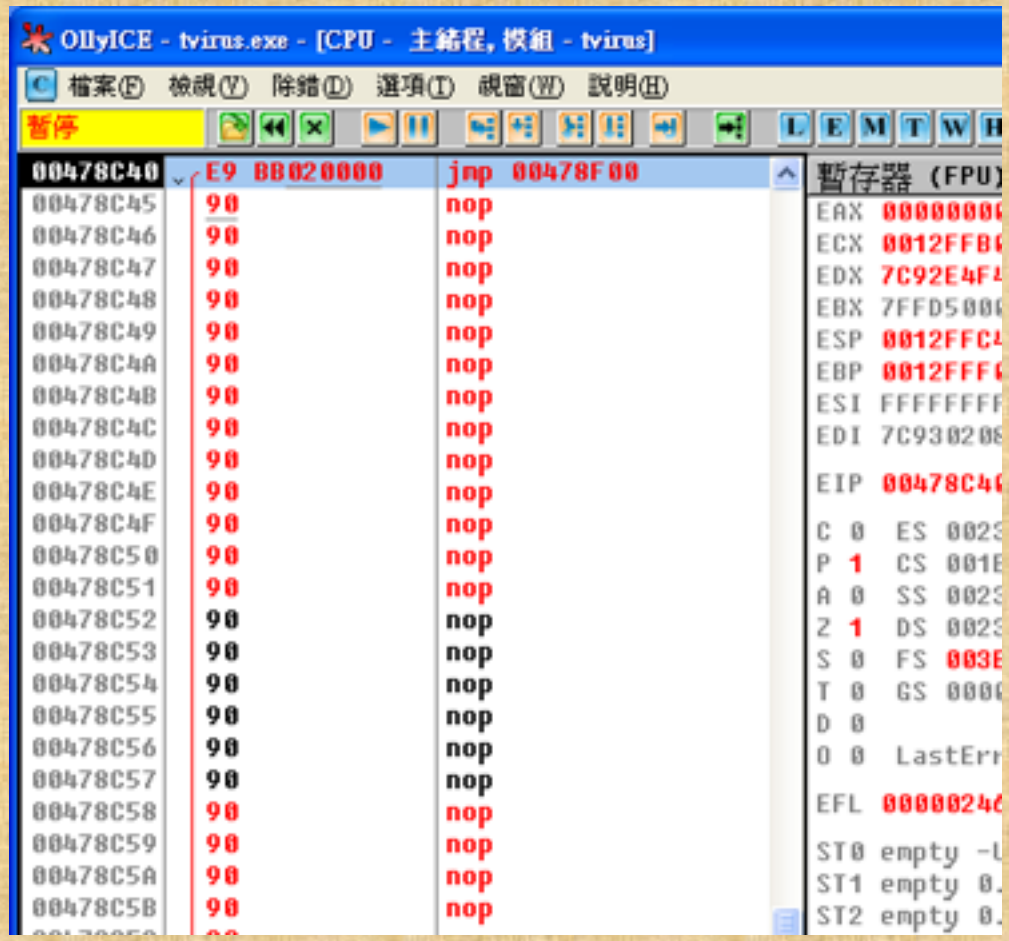
植物大戰殭屍分析修改

ASM惡補!!!!!

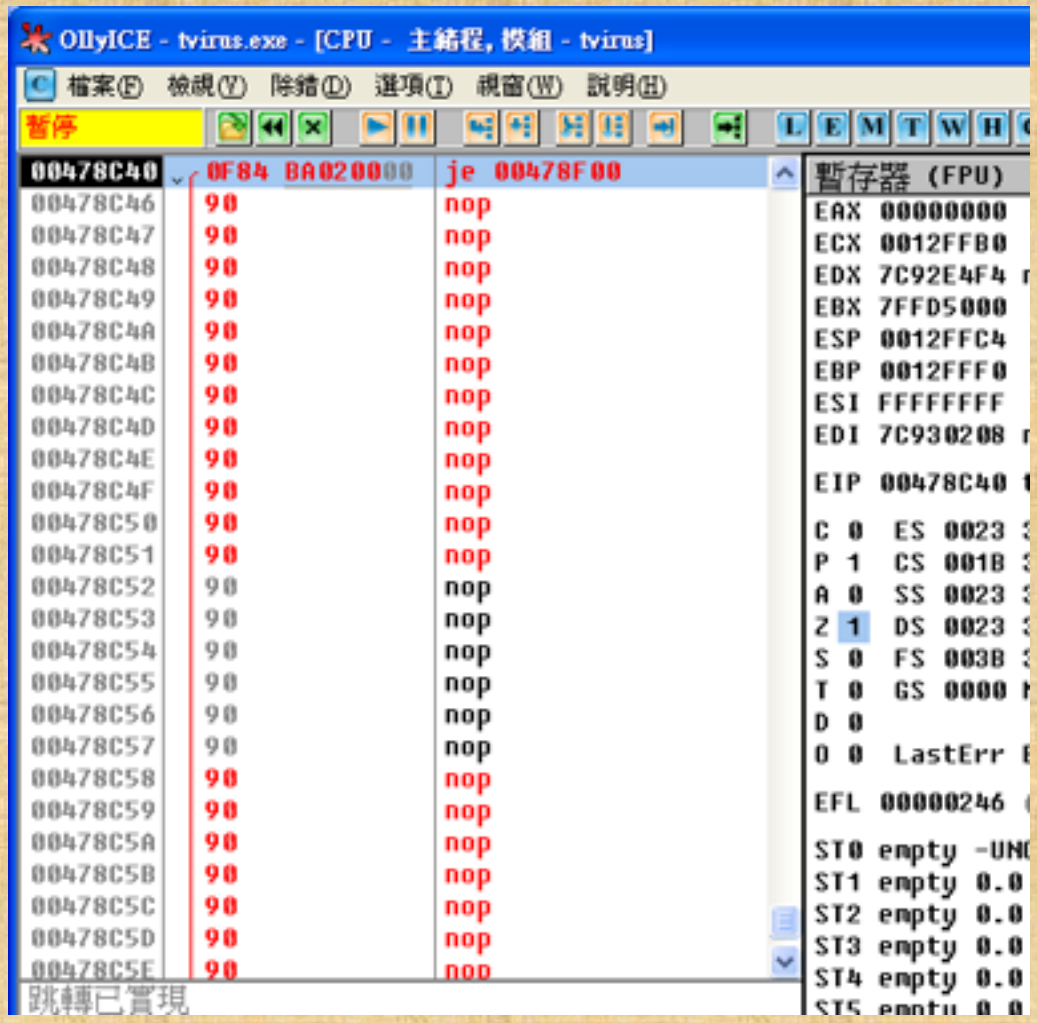
暫存器用途	暫存器名稱
位元暫存器	***EAX,EBX,ECX,EDX***
索引暫存器	***ESI,EDI***
堆疊、基底暫存器	***ESP,EBP***
指位/指標暫存器	***EIP***
旗標暫存器	**AF**：輔助進位旗標 **CF**：進位旗標 **OF**：溢位旗標

指令	用途
jmp 地址	無條件跳轉到某地址
je 地址	如果暫存器***ZF=1***就跳轉
jne 地址	如果暫存器***ZF=0***就跳轉
add 數值***A***,數值***B***	把數值***B***加到數值***A*** 數值***A***可為地址
call 地址	把返回地址壓進堆疊 之後跳轉到地址
mov 內容***A***,內容***B***	把內容***B***複製到內容***A***
cmp 內容***A***,內容***B***	比較地址***A***跟地址***B***的內容,並將結果反映在
nop	不做任何動作

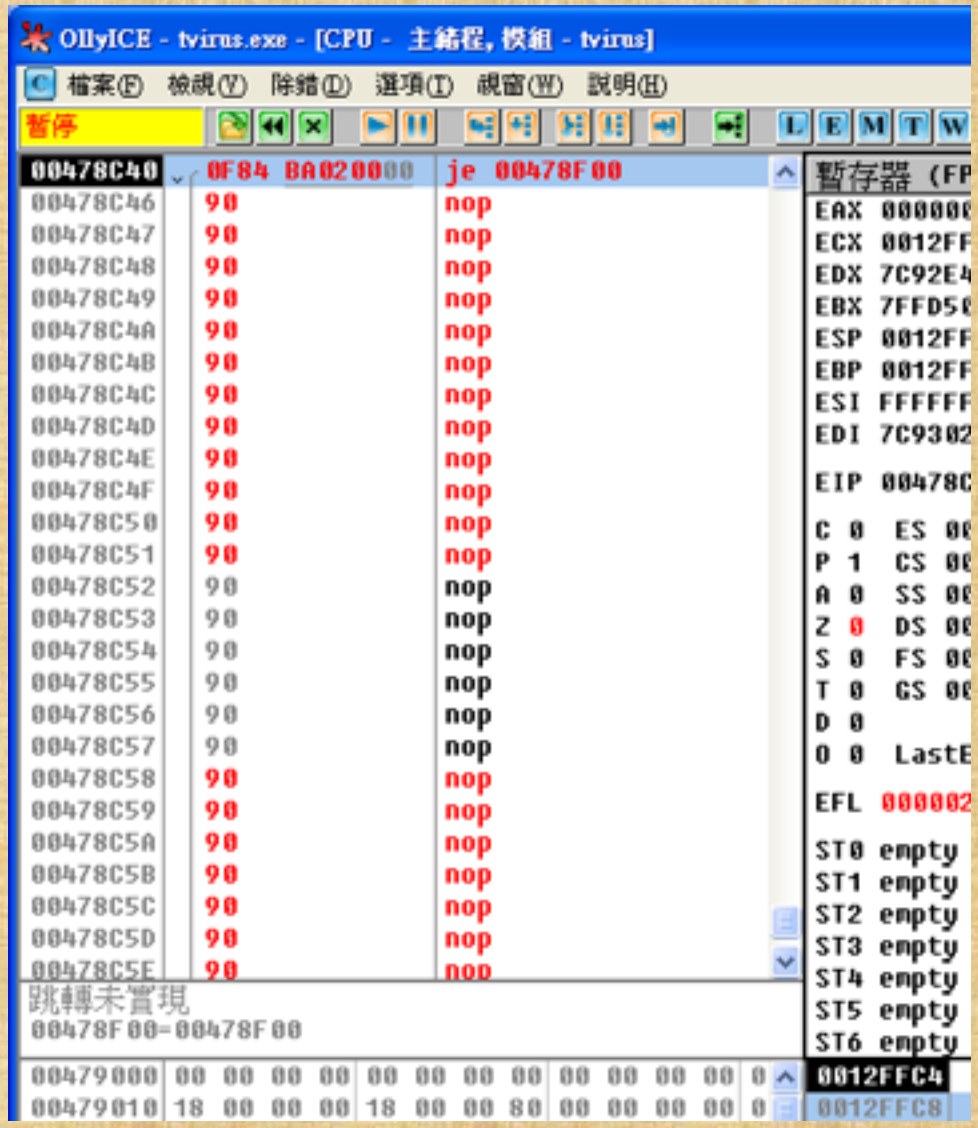
jmp


OllyICE - tvirus.exe - [CPU - 主緒程, 模組 - tvirus]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00478C40 E9 BB020000 jmp 00478F00
00478C45 90 nop
00478C46 90 nop
00478C47 90 nop
00478C48 90 nop
00478C49 90 nop
00478C4A 90 nop
00478C4B 90 nop
00478C4C 90 nop
00478C4D 90 nop
00478C4E 90 nop
00478C4F 90 nop
00478C50 90 nop
00478C51 90 nop
00478C52 90 nop
00478C53 90 nop
00478C54 90 nop
00478C55 90 nop
00478C56 90 nop
00478C57 90 nop
00478C58 90 nop
00478C59 90 nop
00478C5A 90 nop
00478C5B 90 nop
暫存器 (FPU)

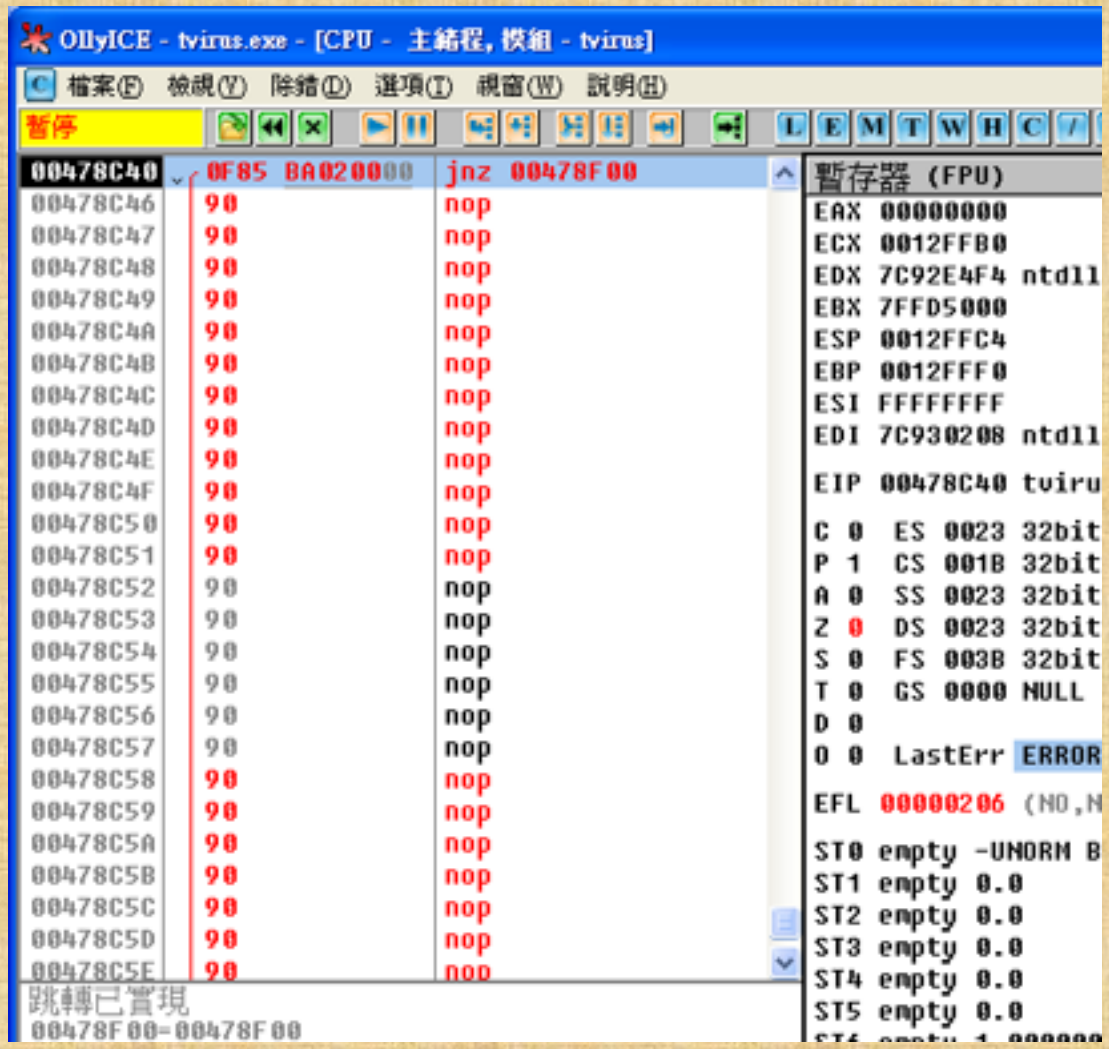
je


OllyICE - tvirus.exe - [CPU - 主緒程, 模組 - tvirus]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00478C40 0F84 BA020000 je 00478F00
00478C46 90 nop
00478C47 90 nop
00478C48 90 nop
00478C49 90 nop
00478C4A 90 nop
00478C4B 90 nop
00478C4C 90 nop
00478C4D 90 nop
00478C4E 90 nop
00478C4F 90 nop
00478C50 90 nop
00478C51 90 nop
00478C52 90 nop
00478C53 90 nop
00478C54 90 nop
00478C55 90 nop
00478C56 90 nop
00478C57 90 nop
00478C58 90 nop
00478C59 90 nop
00478C5A 90 nop
00478C5B 90 nop
00478C5C 90 nop
00478C5D 90 nop
00478C5E 90 nop
跳轉已實現
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4
EBX 7FFD5000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208
EIP 00478C40
C 0 ES 0023
P 1 CS 001B
A 0 SS 0023
Z 1 DS 0023
S 0 FS 003B
T 0 GS 0000
D 0
O 0 LastErr
EFL 00000246
ST0 empty
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0

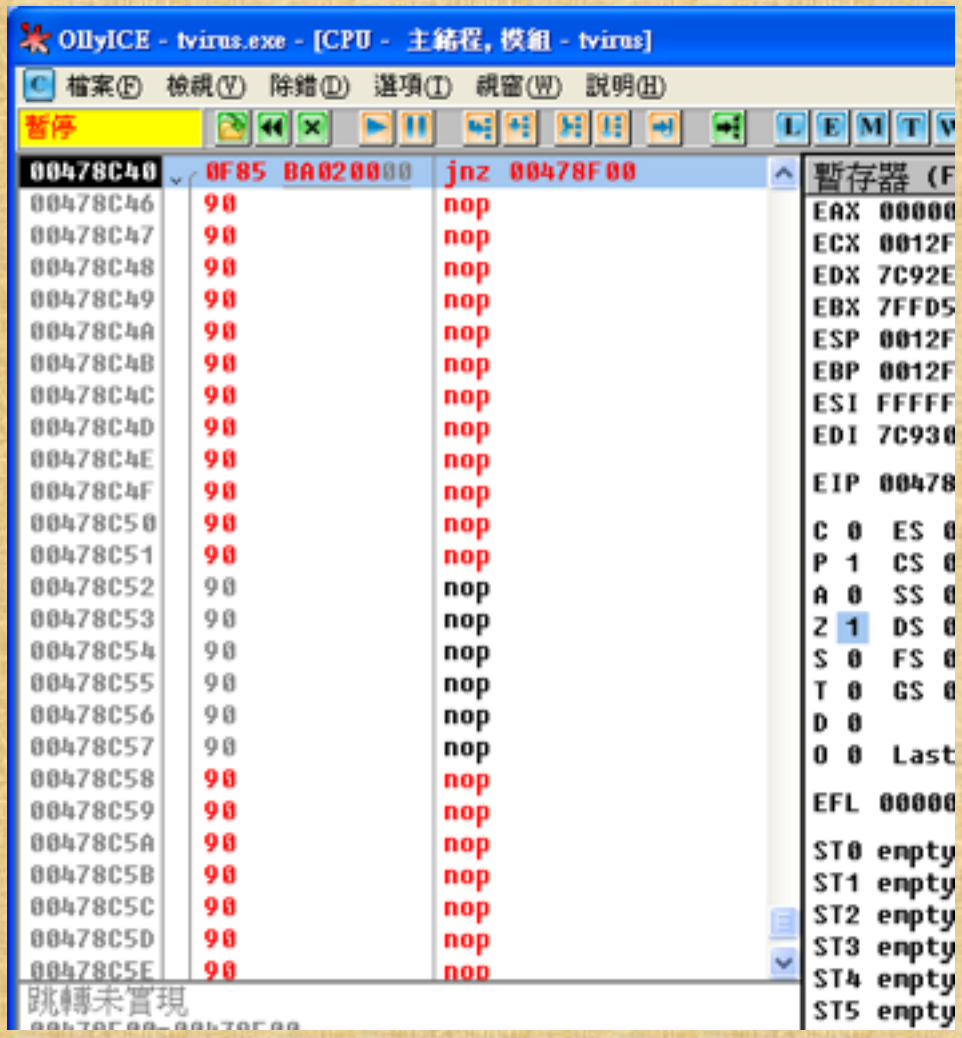
je


OllyICE - tvirus.exe - [CPU - 主緒程, 模組 - tvirus]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00478C40 0F84 BA020000 je 00478F00
00478C46 90 nop
00478C47 90 nop
00478C48 90 nop
00478C49 90 nop
00478C4A 90 nop
00478C4B 90 nop
00478C4C 90 nop
00478C4D 90 nop
00478C4E 90 nop
00478C4F 90 nop
00478C50 90 nop
00478C51 90 nop
00478C52 90 nop
00478C53 90 nop
00478C54 90 nop
00478C55 90 nop
00478C56 90 nop
00478C57 90 nop
00478C58 90 nop
00478C59 90 nop
00478C5A 90 nop
00478C5B 90 nop
00478C5C 90 nop
00478C5D 90 nop
00478C5E 90 nop
跳轉未實現
00478F00-00478F00
00479000 00 00 00 00 00 00 00 00 00 00 00 00
00479010 18 00 00 00 18 00 00 80 00 00 00 00
暫存器 (FP
EAX 000000
ECX 0012FF
EDX 7C92E4
EBX 7FFD50
ESP 0012FF
EBP 0012FF
ESI FFFFFF
EDI 7C9302
EIP 00478C
C 0 ES 00
P 1 CS 00
A 0 SS 00
Z 0 DS 00
S 0 FS 00
T 0 GS 00
D 0
O 0 LastE
EFL 000002
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
0012FFC4
0012FFC8

Jne/jnz


OllyICE - tvirus.exe - [CPU - 主緒程, 模組 - tvirus]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00478C40 0F85 BA020000 jnz 00478F00
00478C46 90 nop
00478C47 90 nop
00478C48 90 nop
00478C49 90 nop
00478C4A 90 nop
00478C4B 90 nop
00478C4C 90 nop
00478C4D 90 nop
00478C4E 90 nop
00478C4F 90 nop
00478C50 90 nop
00478C51 90 nop
00478C52 90 nop
00478C53 90 nop
00478C54 90 nop
00478C55 90 nop
00478C56 90 nop
00478C57 90 nop
00478C58 90 nop
00478C59 90 nop
00478C5A 90 nop
00478C5B 90 nop
00478C5C 90 nop
00478C5D 90 nop
00478C5E 90 nop
跳轉已實現
00478F00-00478F00
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll
EBX 7FFD5000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll
EIP 00478C40 tviru
C 0 ES 0023 32bit
P 1 CS 001B 32bit
A 0 SS 0023 32bit
Z 0 DS 0023 32bit
S 0 FS 003B 32bit
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR
EFL 00000206 (NO,N
ST0 empty -UNORM B
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0

Jne/jnz


OllyICE - tvirus.exe - [CPU - 主緒程, 模組 - tvirus]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00478C40 0F85 BA020000 jnz 00478F00
00478C46 90 nop
00478C47 90 nop
00478C48 90 nop
00478C49 90 nop
00478C4A 90 nop
00478C4B 90 nop
00478C4C 90 nop
00478C4D 90 nop
00478C4E 90 nop
00478C4F 90 nop
00478C50 90 nop
00478C51 90 nop
00478C52 90 nop
00478C53 90 nop
00478C54 90 nop
00478C55 90 nop
00478C56 90 nop
00478C57 90 nop
00478C58 90 nop
00478C59 90 nop
00478C5A 90 nop
00478C5B 90 nop
00478C5C 90 nop
00478C5D 90 nop
00478C5E 90 nop
跳轉未實現
暫存器 (F
EAX 00000
ECX 0012F
EDX 7C92E
EBX 7FFD5
ESP 0012F
EBP 0012F
ESI FFFFF
EDI 7C930
EIP 00478
C 0 ES 0
P 1 CS 0
A 0 SS 0
Z 1 DS 0
S 0 FS 0
T 0 GS 0
D 0
O 0 Last
EFL 00000
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty

讓我小小休息一下QQ

Q&A

逆向工程有分成

1.動態分析
2.靜態分析

動態分析

軟體執行中,邊執行邊分析,方便觀　察暫存器的變化

常用工具:**OLLYDBG, Cheat engine**

靜態分析

直接閱讀他的組合語言來分析那段組合語言的用途

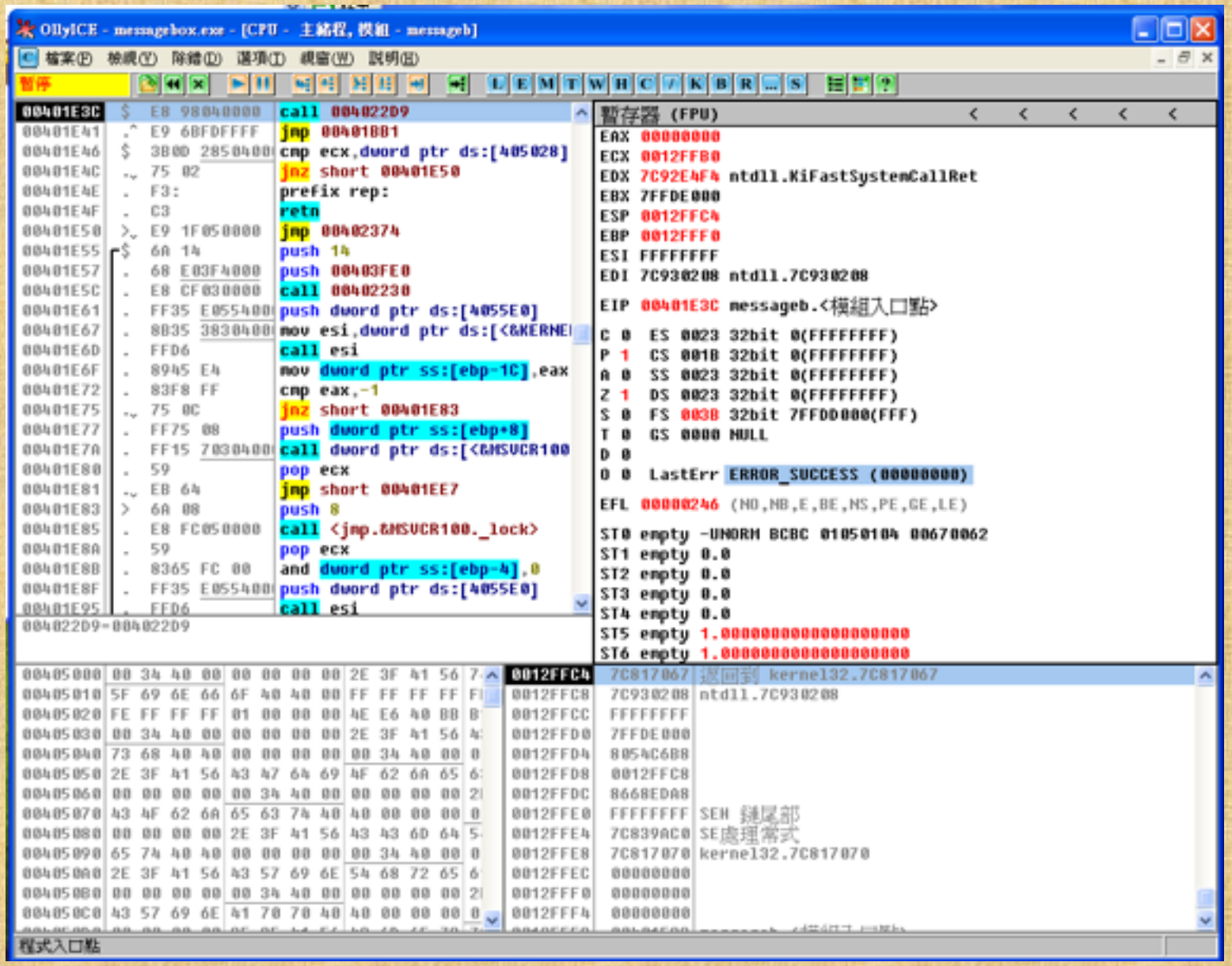
常用工具:**IDA PRO**

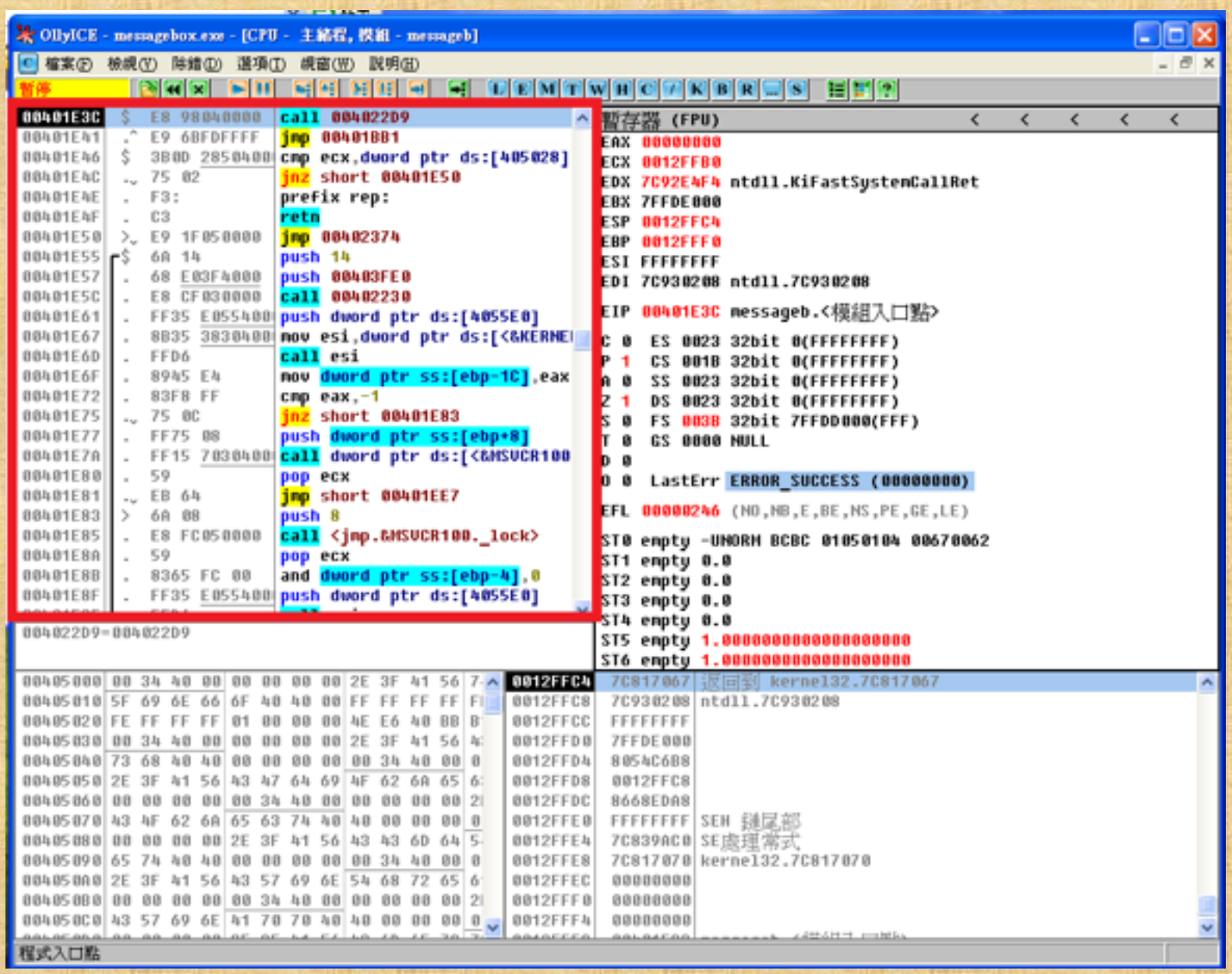
1.OLLYDBG實作演練

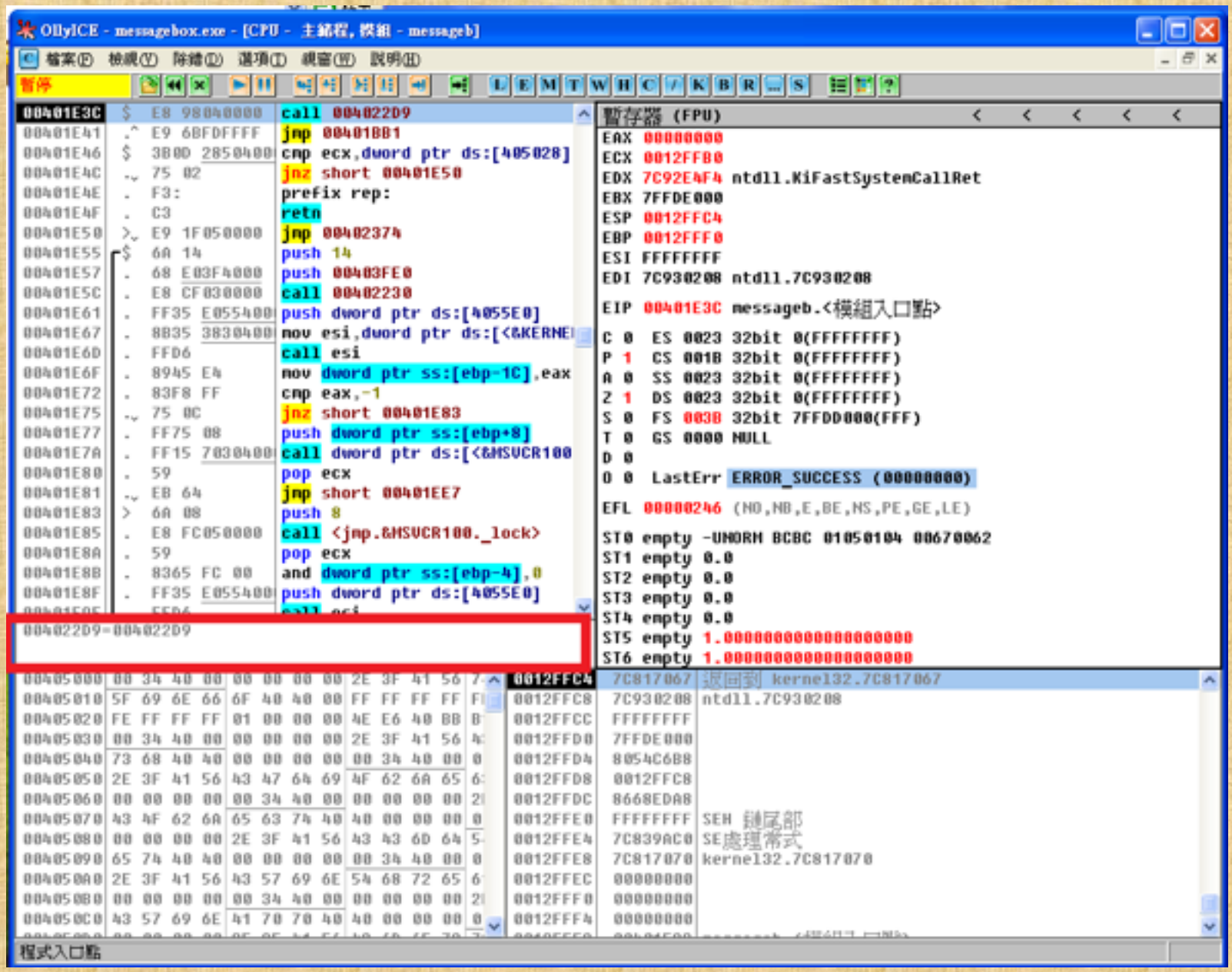
OLLYDBG介紹

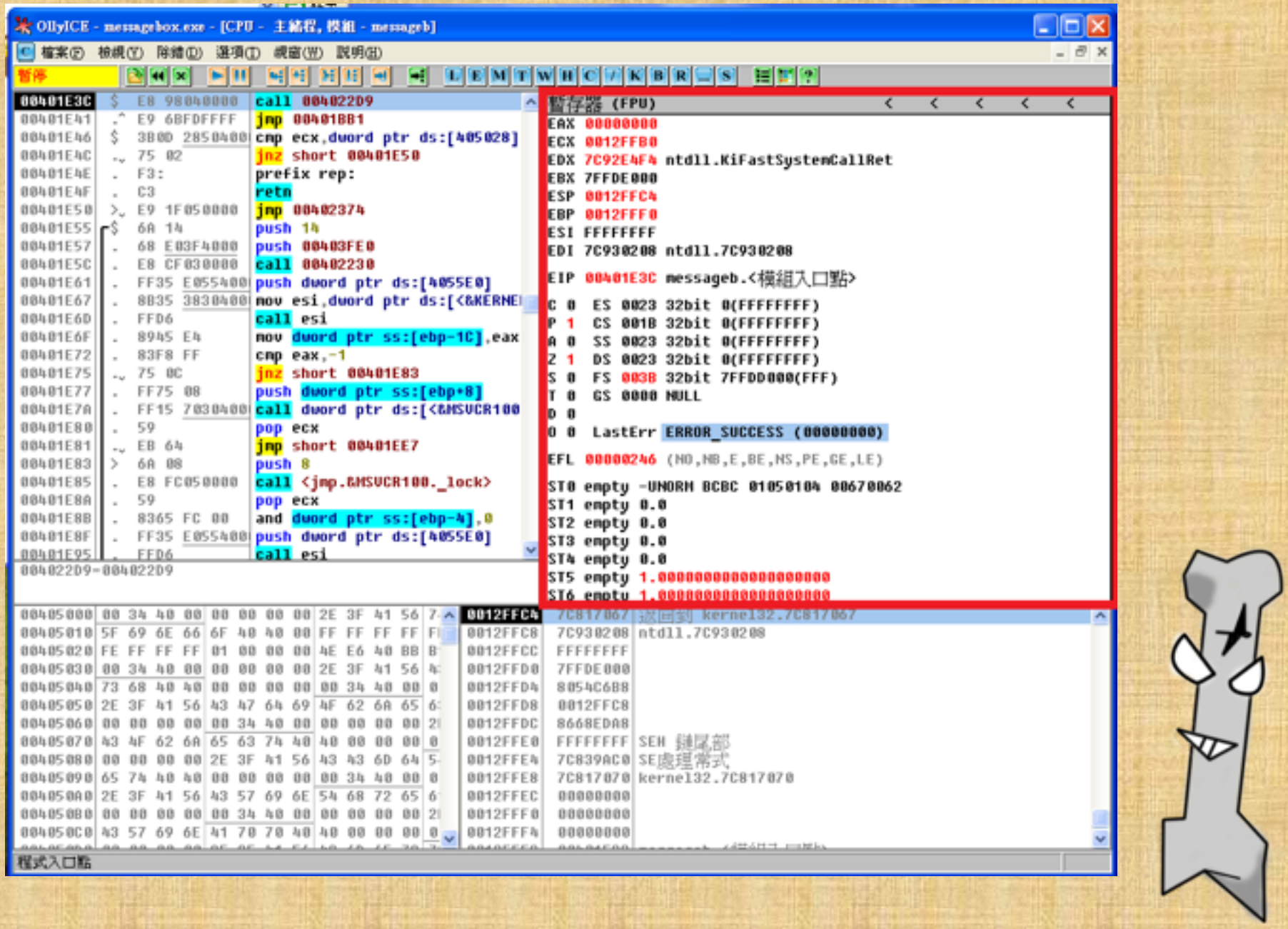
OllyDbg 是一種具有可視化介面的 32 位彙編-分析偵錯器。它的特別之處在於可以在沒有來源碼時解決問題，並且可以處理其它編譯器無法解決的難題。

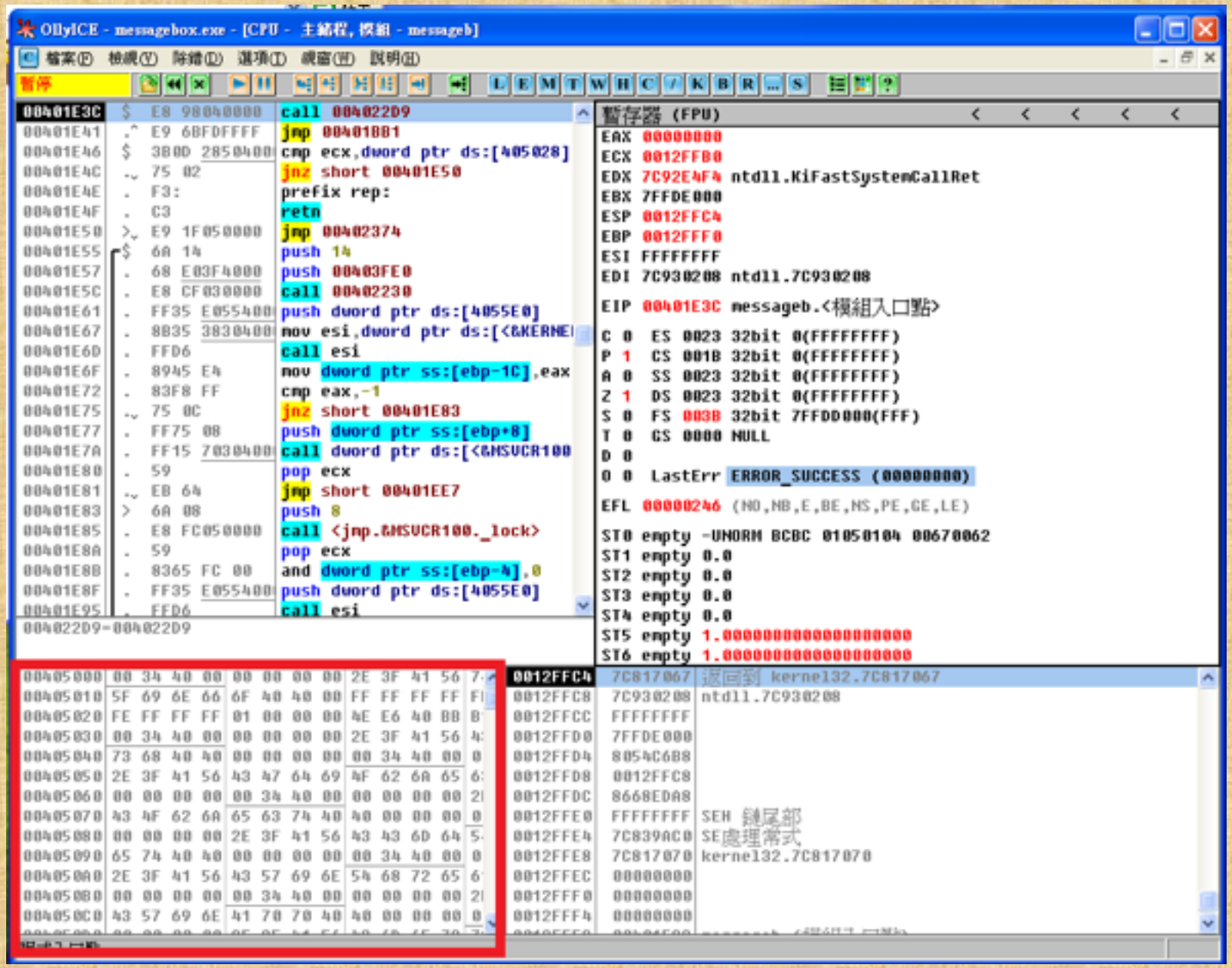
OLLYDBG介面介紹

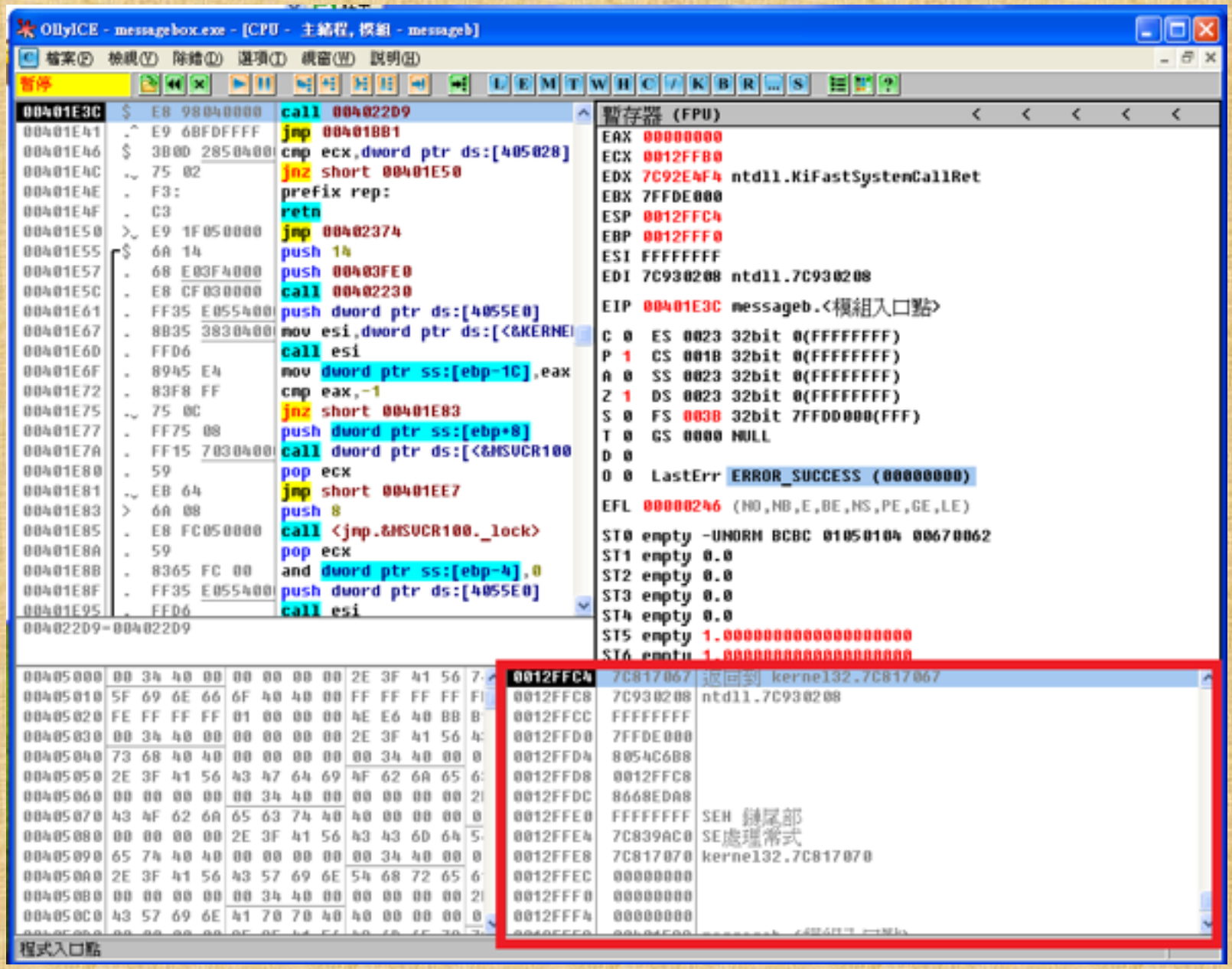

OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401881
00401E46 $ 3B0D 2850400 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 $ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E055400 push dword ptr ds:[4055E0]
00401E67 . 8B35 3830400 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 7030400 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E055400 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209-00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點

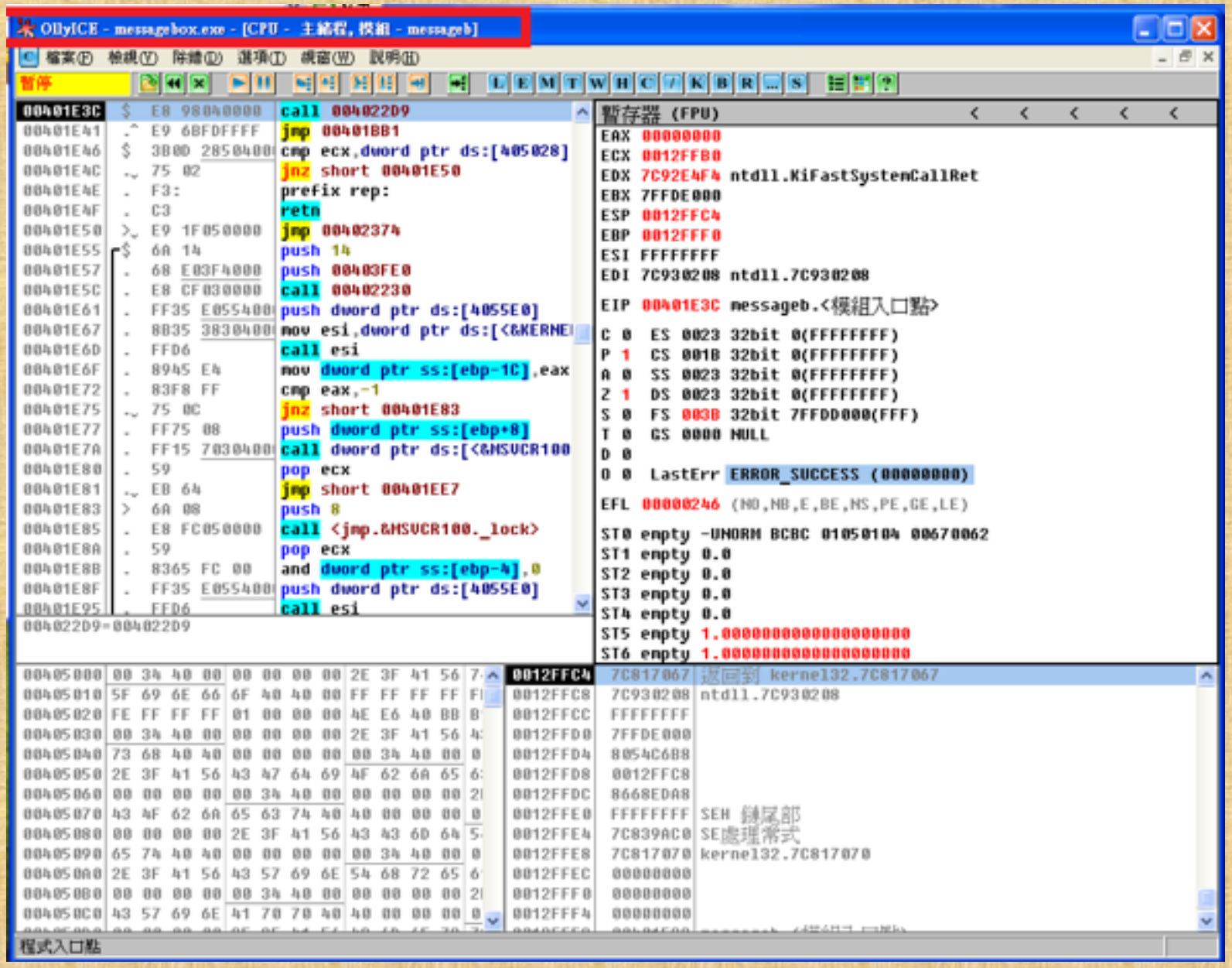

OllyICE - messagebox.exe - [CPU - 主線程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(I) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 2850400 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E055400 push dword ptr ds:[4055E0]
00401E67 . 8B35 3830400 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 7030400 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E055400 push dword ptr ds:[4055E0]
00402209=00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點

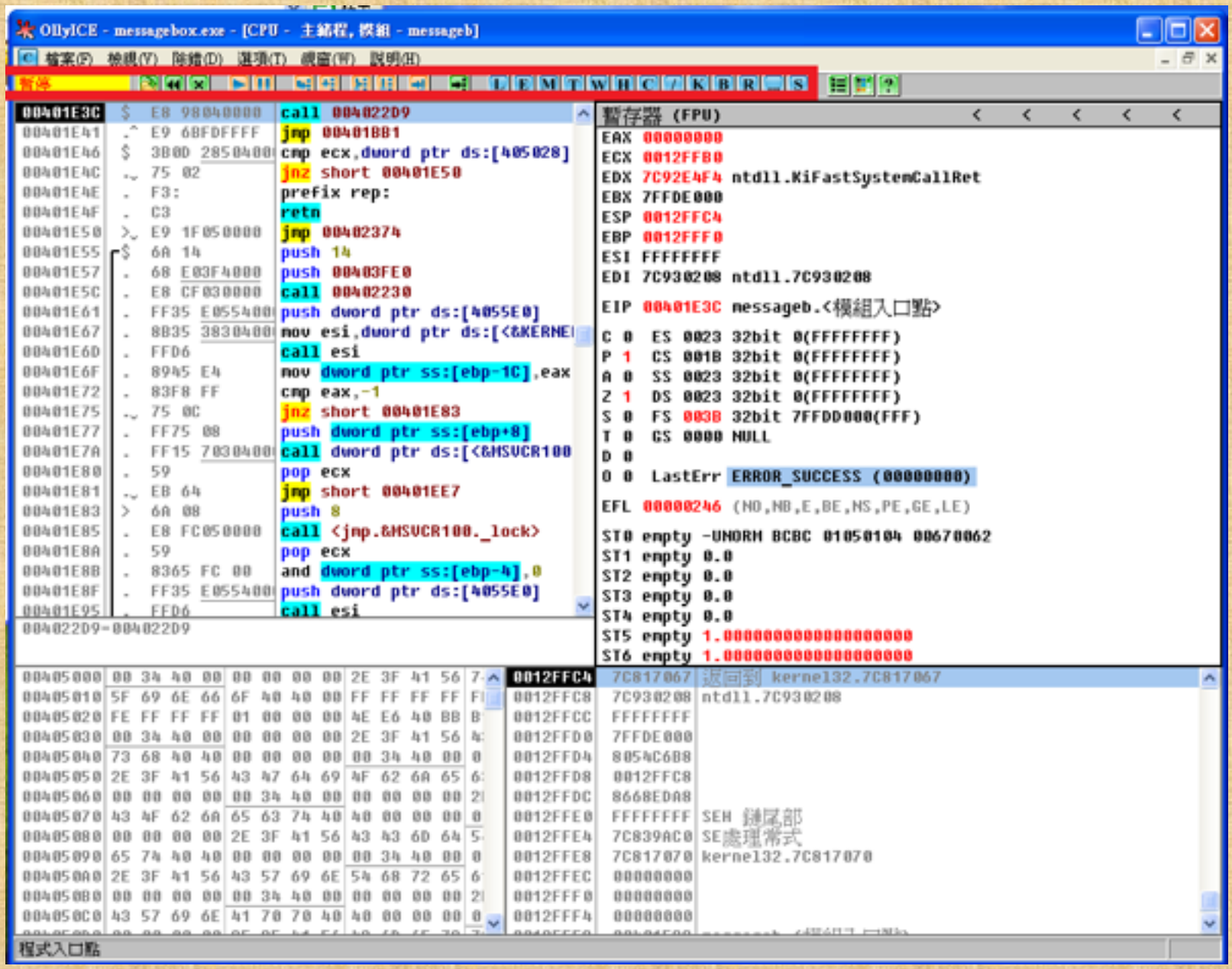

OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 2850400 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E055400 push dword ptr ds:[4055E0]
00401E67 . 8B35 3830400 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 7030400 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E055400 push dword ptr ds:[4055E0]
00402209=00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點

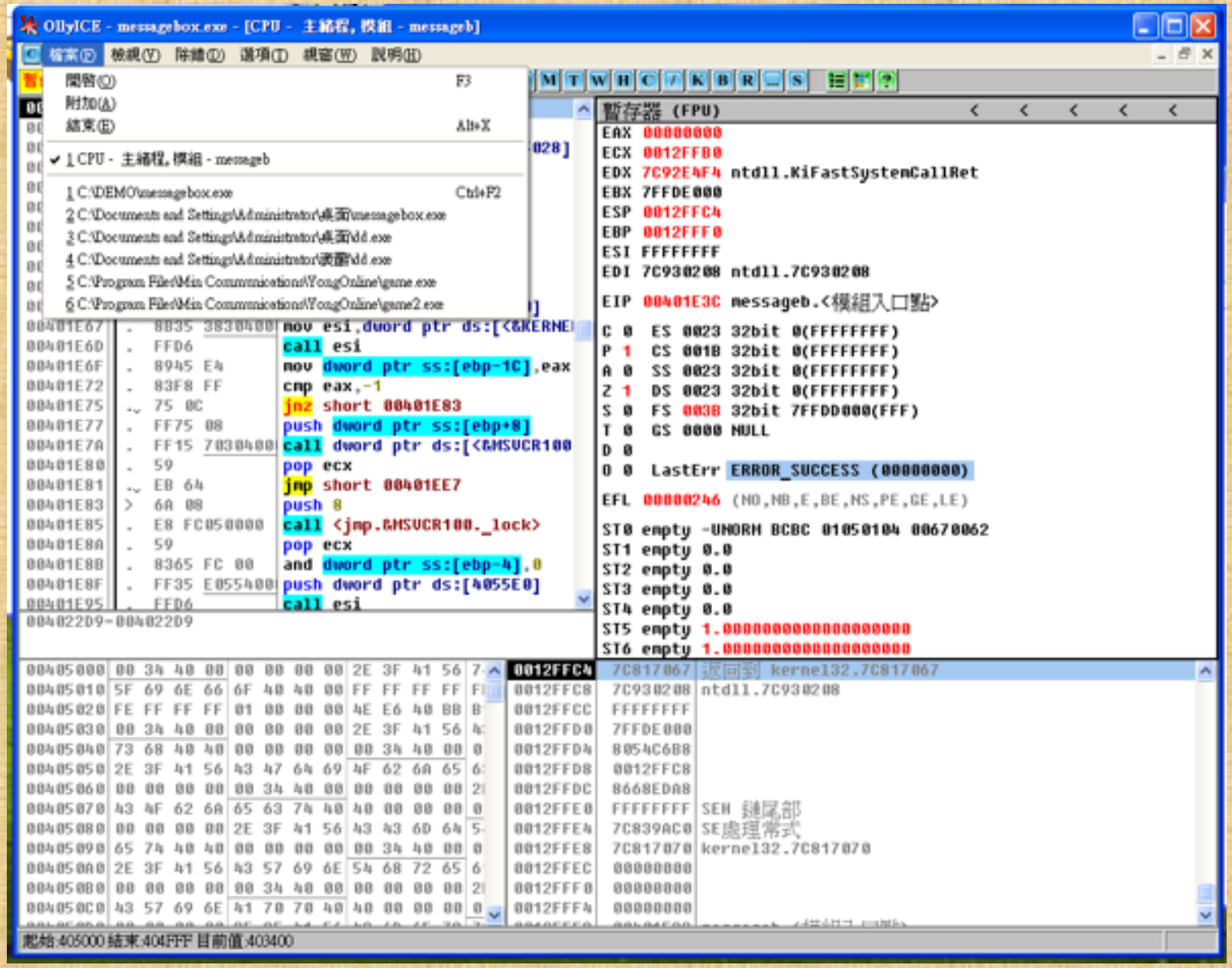

OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 2850400 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E055400 push dword ptr ds:[4055E0]
00401E67 . 8B35 3830400 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 7030400 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E055400 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209=00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 0105010A 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點

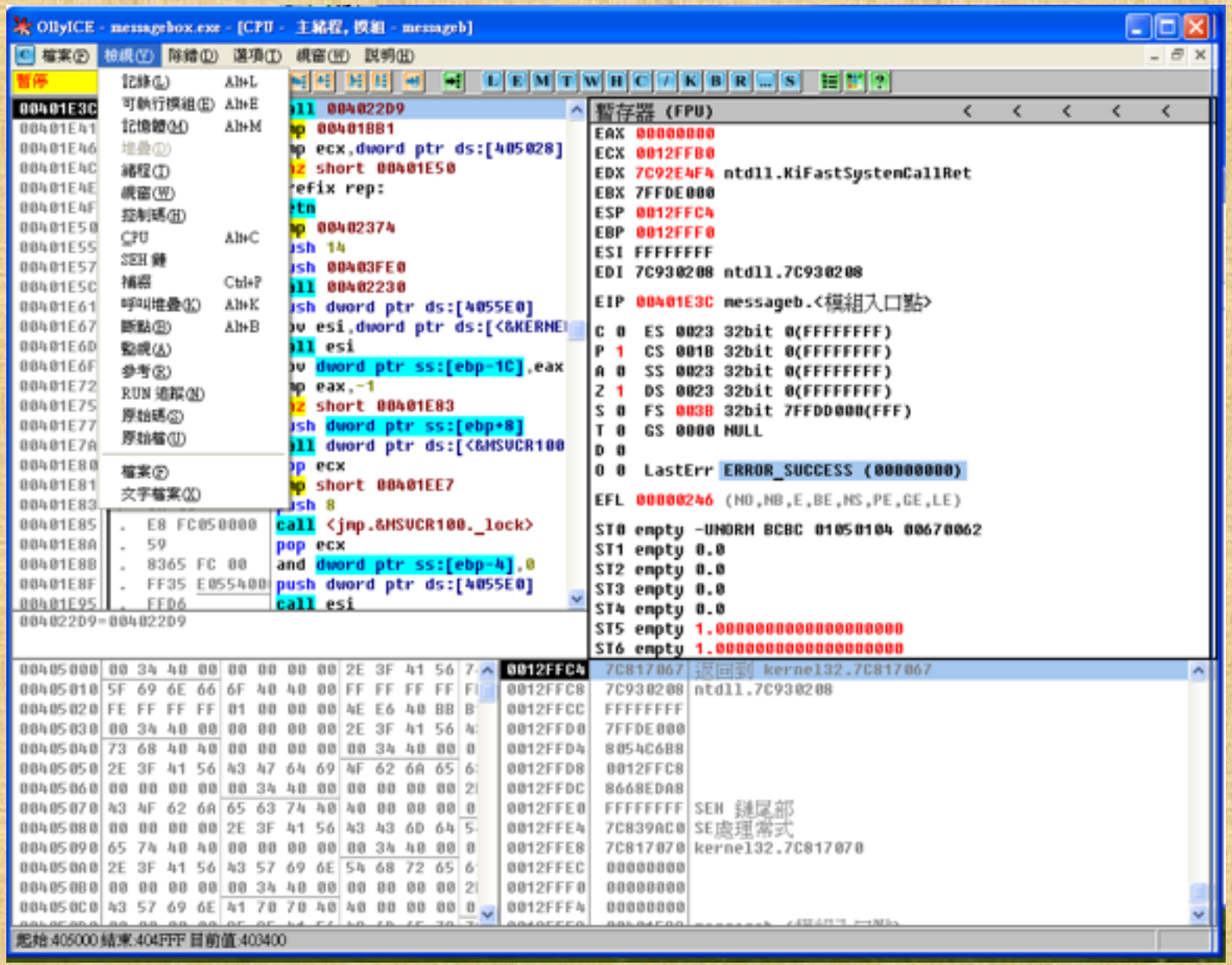

OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 28504000 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E0554000 push dword ptr ds:[4055E0]
00401E67 . 8B35 38304000 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 70304000 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E0554000 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209-00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 0105010400670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C688
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000

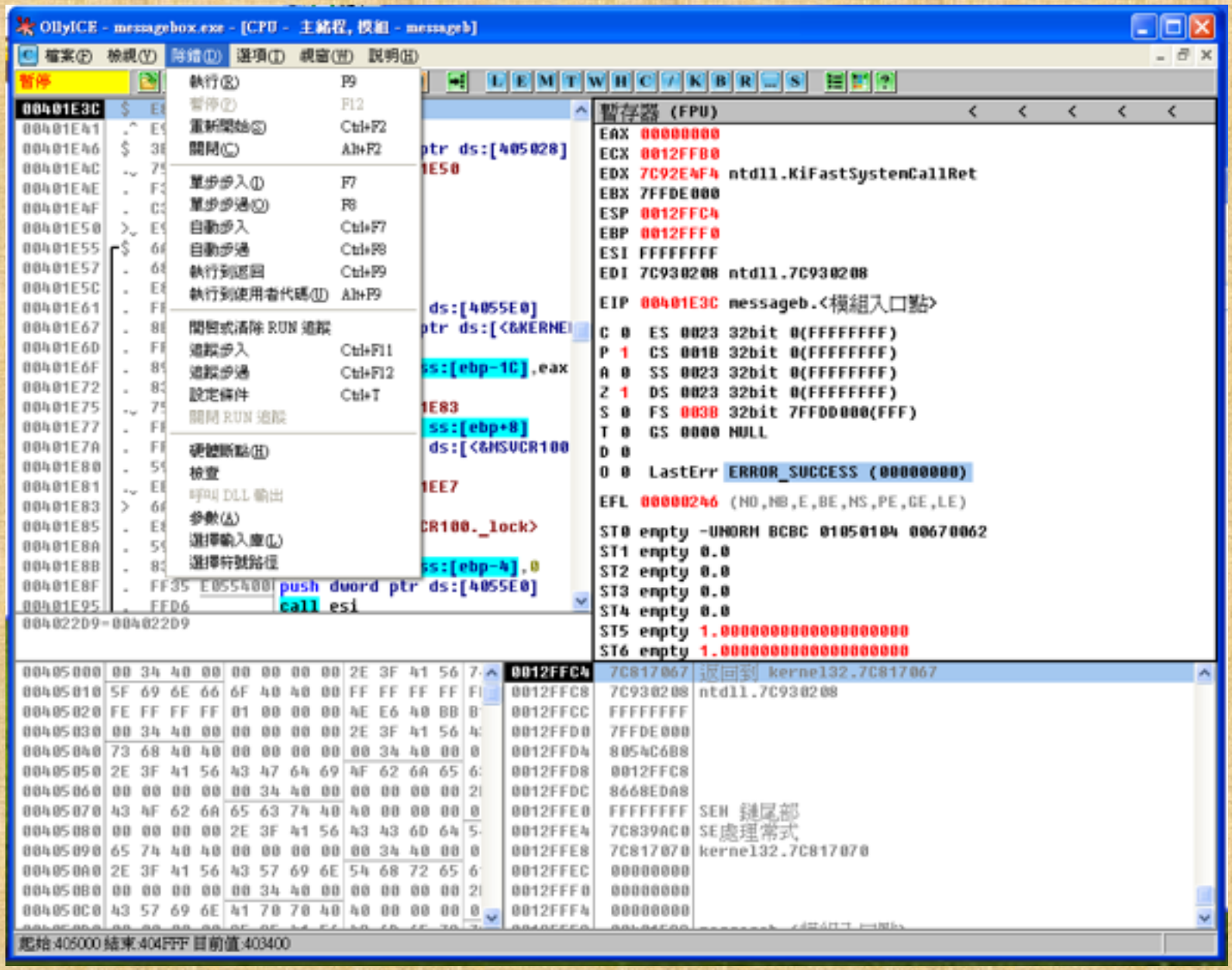

OllyICE - messagebox.exe - [CPU - 主結程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 2850400 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E0554000 push dword ptr ds:[4055E0]
00401E67 . 8B35 3830400 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 7030400 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E0554000 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209-00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.0000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點

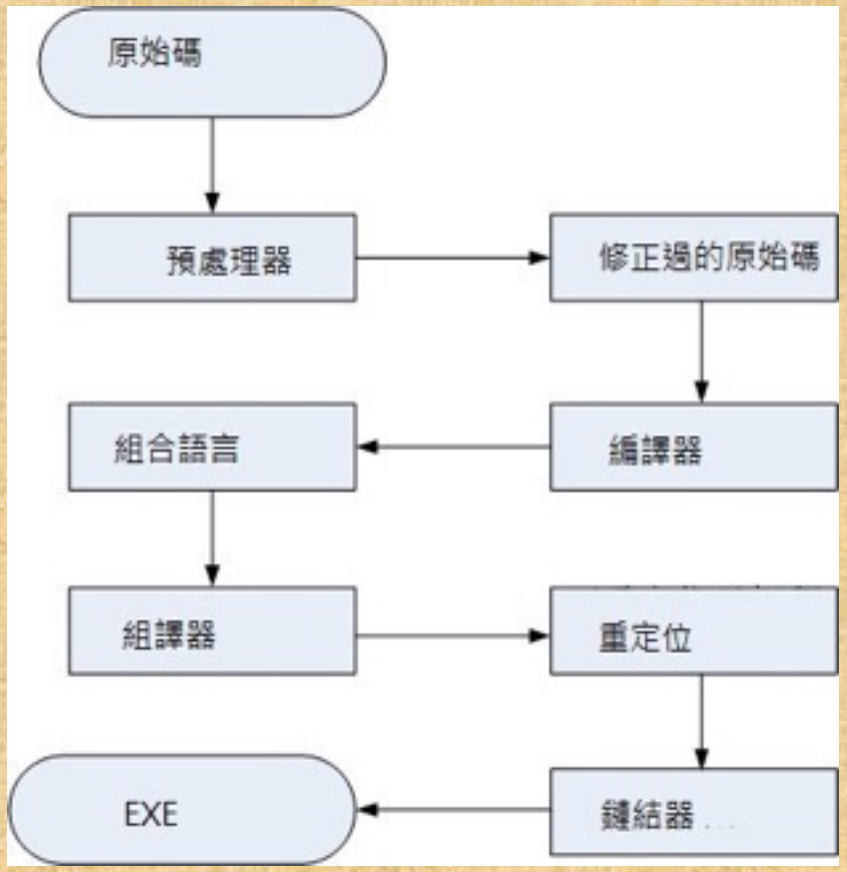

OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 6BFDFFFF jmp 00401BB1
00401E46 $ 3B0D 28504000 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E0554000 push dword ptr ds:[4055E0]
00401E67 . 8B35 38304000 mov esi,dword ptr ds:[<&KERNEL
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 70304000 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E0554000 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209=00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BC8C 0105010A 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C688
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點


OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
00401E3C $ E8 98040000 call 00402209
00401E41 .^ E9 68FDFFFF jmp 00401BB1
00401E46 $ 3B0D 28504000 cmp ecx,dword ptr ds:[405028]
00401E4C .v 75 02 jnz short 00401E50
00401E4E . F3: prefix rep:
00401E4F . C3 retn
00401E50 >v E9 1F050000 jmp 00402374
00401E55 r$ 6A 14 push 14
00401E57 . 68 E03F4000 push 00403FE0
00401E5C . E8 CF030000 call 00402230
00401E61 . FF35 E0554000 push dword ptr ds:[4055E0]
00401E67 . 8B35 38304000 mov esi,dword ptr ds:[<&KERNE
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 .v 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 70304000 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 .v EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E0554000 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209-00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C688
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
程式入口點


OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
開啓(O) F3
附加(A)
結束(E) Alt+X
1 CPU - 主緒程, 模組 - messageb
1 C:\DEMO\messagebox.exe Ctrl+F2
2 C:\Documents and Settings\Administrator\桌面\messagebox.exe
3 C:\Documents and Settings\Administrator\桌面\dd.exe
4 C:\Documents and Settings\Administrator\桌面\dd.exe
5 C:\Program Files\Min Communications\YongOnline\game.exe
6 C:\Program Files\Min Communications\YongOnline\game2.exe
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM 8CBC 0105010400670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
00401E67 . 8B35 38304000 mov esi,dword ptr ds:[<&KERNEL
00401E6D . FFD6 call esi
00401E6F . 8945 E4 mov dword ptr ss:[ebp-1C],eax
00401E72 . 83F8 FF cmp eax,-1
00401E75 . 75 0C jnz short 00401E83
00401E77 . FF75 08 push dword ptr ss:[ebp+8]
00401E7A . FF15 70304000 call dword ptr ds:[<&MSVCR100
00401E80 . 59 pop ecx
00401E81 . EB 64 jmp short 00401EE7
00401E83 > 6A 08 push 8
00401E85 . E8 FC050000 call <jmp.&MSVCR100._lock>
00401E8A . 59 pop ecx
00401E8B . 8365 FC 00 and dword ptr ss:[ebp-4],0
00401E8F . FF35 E0554000 push dword ptr ds:[4055E0]
00401E95 . FFD6 call esi
00402209-00402209
00405000 00 34 40 00 00 00 00 00 2E 3F A1 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F A1 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F A1 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F A1 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F A1 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E A1 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C6B8
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
起始 405000 結束 404FFF 目前值 403400


OllyICE - messagebox.exe - [CPU - 主線程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
記錄(L) Alt+L
可執行模組(E) Alt+E
記憶體(M) Alt+M
堆疊(D)
線程(T)
視窗(W)
控制碼(H)
CPU Alt+C
SEH 鏈
補綴 Ctrl+P
呼叫堆疊(K) Alt+K
斷點(B) Alt+B
監視(A)
參考(R)
RUN 追踪(N)
原始碼(S)
原始檔(U)
檔案(F)
文字檔案(X)
00401E3C
00401E41
00401E46
00401E4C
00401E4E
00401E4F
00401E50
00401E55
00401E57
00401E5C
00401E61
00401E67
00401E6D
00401E6F
00401E72
00401E75
00401E77
00401E7A
00401E80
00401E81
00401E83
00401E85
00401E8A
00401E8B
00401E8F
00401E95
00402374
00402230
00401EE7
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
00402209-00402209
0012FFC4
0012FFC8
0012FFCC
0012FFD0
0012FFD4
0012FFD8
0012FFDC
0012FFE0
0012FFE4
0012FFE8
0012FFEC
0012FFF0
0012FFF4
7C817067 返回到 kernel32.7C817067
7C930208 ntdll.7C930208
FFFFFFFF
7FFDE000
SEH 鏈尾部
SE處理常式
7C817070 kernel32.7C817070
起始:406000 結束:404FFF 目前值:403400


OllyICE - messagebox.exe - [CPU - 主緒程, 模組 - messageb]
檔案(F) 檢視(V) 除錯(D) 選項(T) 視窗(W) 說明(H)
暫停
執行(R) F9
暫停(Z) F12
重新開始(S) Ctrl+F2
關閉(C) Alt+F2
單步步入(I) F7
單步步過(O) F8
自動步入 Ctrl+F7
自動步過 Ctrl+F8
執行到返回 Ctrl+F9
執行到使用者代碼(U) Alt+F9
開啟或清除 RUN 追踪
追踪步入 Ctrl+F11
追踪步過 Ctrl+F12
設定條件 Ctrl+T
關閉 RUN 追踪
硬體斷點(H)
檢查
呼叫 DLL 輸出
參數(A)
選擇輸入庫(L)
選擇符號路徑
00401E3C
00401E41
00401E46
00401E4C
00401E4E
00401E4F
00401E50
00401E55
00401E57
00401E5C
00401E61
00401E67
00401E6D
00401E6F
00401E72
00401E75
00401E77
00401E7A
00401E80
00401E81
00401E83
00401E85
00401E8A
00401E8B
00401E8F
00401E95
ptr ds:[405028]
1E50
ds:[4055E0]
ptr ds:[<&KERNEL
ss:[ebp-1C],eax
1E83
ss:[ebp+8]
ds:[<&MSVCR100
1EE7
CR100._lock>
ss:[ebp-4],0
push dword ptr ds:[4055E0]
call esi
00402209=00402209
暫存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930208 ntdll.7C930208
EIP 00401E3C messageb.<模組入口點>
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 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM BCBC 01050104 00670062
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
00405000 00 34 40 00 00 00 00 00 2E 3F 41 56
00405010 5F 69 6E 66 6F 40 40 00 FF FF FF FF
00405020 FE FF FF FF 01 00 00 00 4E E6 40 BB
00405030 00 34 40 00 00 00 00 00 2E 3F 41 56
00405040 73 68 40 40 00 00 00 00 00 34 40 00
00405050 2E 3F 41 56 43 47 64 69 4F 62 6A 65
00405060 00 00 00 00 00 34 40 00 00 00 00 00
00405070 43 4F 62 6A 65 63 74 40 40 00 00 00
00405080 00 00 00 00 2E 3F 41 56 43 43 6D 64
00405090 65 74 40 40 00 00 00 00 00 34 40 00
004050A0 2E 3F 41 56 43 57 69 6E 54 68 72 65
004050B0 00 00 00 00 00 34 40 00 00 00 00 00
004050C0 43 57 69 6E 41 70 70 40 40 00 00 00
0012FFC4 7C817067 返回到 kernel32.7C817067
0012FFC8 7C930208 ntdll.7C930208
0012FFCC FFFFFFFF
0012FFD0 7FFDE000
0012FFD4 8054C688
0012FFD8 0012FFC8
0012FFDC 8668EDA8
0012FFE0 FFFFFFFF SEH 鏈尾部
0012FFE4 7C839AC0 SE處理常式
0012FFE8 7C817070 kernel32.7C817070
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
起始:405000 結束:404FFF 目前值:403400


原始碼
預處理器
修正過的原始碼
組合語言
編譯器
組譯器
重定位
EXE
鏈結器

MessageBoxA(NULL,”標題”,”內容”,NULL);

```
push 0
push 內容
push 標題
push 0
CALL MessageBoxA
```

```
If(key == 123){
        ::MessageBoxA(NULL,”標題”,”註冊成功”,NULL);
}
else{
        ::MessageBoxA(NULL,”標題”,”註冊失敗”,NULL);
}
```

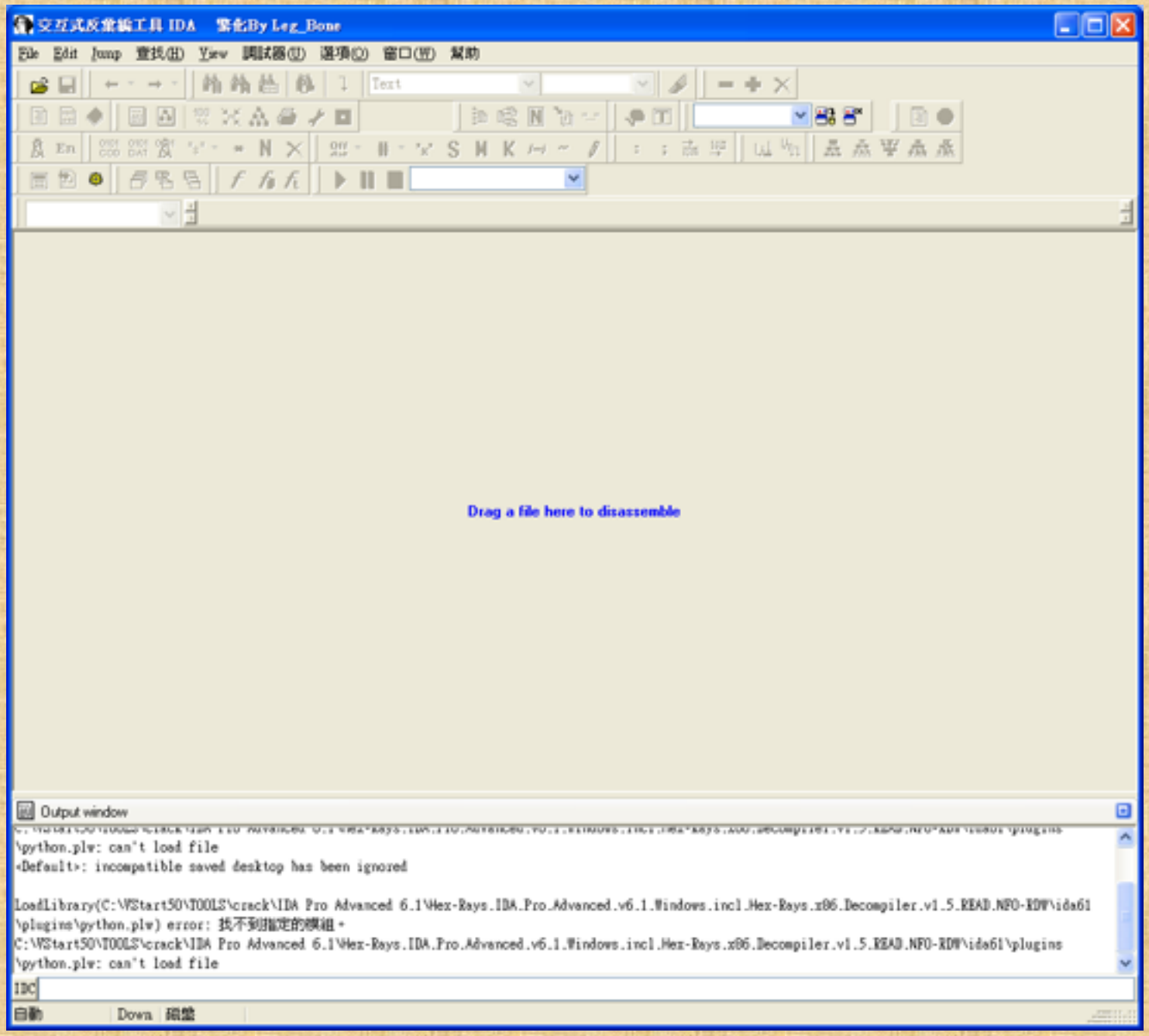
實際破解DEMO

實作時間.....

讓我小小休息一下QQ

Q&A

2.IDA PRO實作演練


交互式反彙編工具 IDA 漢化By Leg_Bone
File Edit Jump 查找(H) View 調試器(D) 選項(O) 窗口(W) 幫助
Text
Drag a file here to disassemble
Output window
\python.plw: can't load file
<Default>: incompatible saved desktop has been ignored
LoadLibrary(C:\VStart50\TOOLS\crack\IDA Pro Advanced 6.1\Hex-Rays.IDA.Pro.Advanced.v6.1.Windows.incl.Hex-Rays.x86.Decompiler.v1.5.READ.NFO-RDW\ida61\plugins\python.plw) error: 找不到指定的模組。
C:\VStart50\TOOLS\crack\IDA Pro Advanced 6.1\Hex-Rays.IDA.Pro.Advanced.v6.1.Windows.incl.Hex-Rays.x86.Decompiler.v1.5.READ.NFO-RDW\ida61\plugins\python.plw: can't load file
IDC
自動
Down
磁盤

交互式反彙編工具 IDA　繁化By Leg_Bone

File Edit Jump 查找(H) View 調試器(D) 選項(O) 窗口(W) 幫助

Drag a file here to disassemble

Output window

\python.plw: can't load file
<Default>: incompatible saved desktop has been ignored

LoadLibrary(C:\VStart50\TOOLS\crack\IDA Pro Advanced 6.1\Hex-Rays.IDA.Pro.Advanced.v6.1.Windows.incl.Hex-Rays.x86.Decompiler.v1.5.READ.NFO-RDW\ida61\plugins\python.plw) error: 找不到指定的模組。
C:\VStart50\TOOLS\crack\IDA Pro Advanced 6.1\Hex-Rays.IDA.Pro.Advanced.v6.1.Windows.incl.Hex-Rays.x86.Decompiler.v1.5.READ.NFO-RDW\ida61\plugins\python.plw: can't load file

IDC

自動　Down　鍵盤

實際破解DEMO

實作時間.....

讓我小小休息一下QQ

Q&A

3.Cheat engine實作演練


Cheat Engine 5.5
File Edit Process Help
No Process Selected
Found: 0
第一次搜尋
第二次以後搜尋
First Scan
Next Scan
Undo scan
Settings
Address
Value
選擇要修改的程式
Value:
Hex
(搜尋數值輸入區)
Scan type: Exact Value
Value type: 4 Bytes
搜尋型態：
一般數值
大於
小於
在…之間
未知數
(搜尋到的位址區)
數值型態：
byte
2bytes
4bytes
float
double
...
等等
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
觀看記憶體編輯
Memory view
手動加入表格
Add address manually
Frozen
Description
Address
Type
Value
(表格區)
飛仔的天地 - 遊戲修改教學網
http://blog.xuite.net/kenking2005/blog
Advanced options
?

一套強大到爆炸的工具!!!!

一套工具可以.....

1.找數值

2.找指針/偏移

3.找中文(超重要TAT)

4.找出訪問的地址

5.加速

6.有內鑲ASM的腳本語言

所以我們要定位出人物血量就必須要找出最上層的CLASS

再來,開始示範上面那些功能

今天就拿它來開刀.....

植物大戰殭屍

實際破解DEMO

實作時間.....

讓我小小休息一下QQ

Q&A

為什麼我要講這麼多工具呢?

怎麼大幅度加快分析效率?

組合技!!!!

逆向冷知識

每種語言的入口點都不一樣

Microsoft Visual C++ 6.0

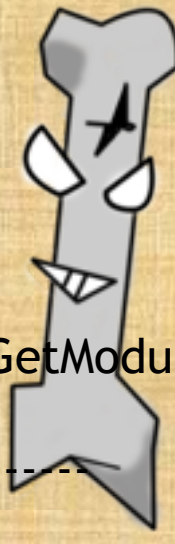
```
00496EB8 >/$  55          PUSH EBP                              ;  (初始 cpu 选择)
00496EB9  |.  8BEC        MOV EBP,ESP
00496EBB  |.  6A FF       PUSH -1
00496EBD  |.  68 40375600 PUSH Screensh.00563740
00496EC2  |.  68 8CC74900 PUSH Screensh.0049C78C                 ;  SE 处理程序安
00496EC7  |.  64:A1 0000000>MOV EAX,DWORD PTR FS:[0]
00496ECD  |.  50          PUSH EAX
00496ECE  |.  64:8925 00000>MOV DWORD PTR FS:[0],ESP
00496ED5  |.  83EC 58     SUB ESP,58
```

Microsoft Visual Basic 5.0 / 6.0

```
00401166   - FF25 6C104000 JMP DWORD PTR DS:[<&MSVBVM60.#100>]   ;
MSVBVM60.ThunRTMain
0040116C >   68 147C4000     PUSH PACKME.00407C14
00401171 E8 F0FFFFFF     CALL <JMP.&MSVBVM60.#100>
00401176 0000         ADD BYTE PTR DS:[EAX],AL
00401178 0000         ADD BYTE PTR DS:[EAX],AL
0040117A 0000         ADD BYTE PTR DS:[EAX],AL
0040117C 3000         XOR BYTE PTR DS:[EAX],AL
```

BC++

```
0040163C > $ /EB 10      JMP SHORT BCLOCK.0040164E
0040163E     |66         DB 66                          ;  CHAR 'f'
0040163F     |62         DB 62                          ;  CHAR 'b'
00401640     |3A         DB 3A                          ;  CHAR ':'
00401641     |43         DB 43                          ;  CHAR 'C'
00401642     |2B         DB 2B                          ;  CHAR '+'
00401643     |2B         DB 2B                          ;  CHAR '+'
00401644     |48         DB 48                          ;  CHAR 'H'
00401645     |4F         DB 4F                          ;  CHAR 'O'
00401646     |4F         DB 4F                          ;  CHAR 'O'
00401647     |4B         DB 4B                          ;  CHAR 'K'
00401648     |90         NOP
00401649     |E9         DB E9
0040164A . |98E04E00    DD OFFSET BCLOCK.___CPPdebugHook
0040164E > \A1 8BE04E00 MOV EAX,DWORD PTR DS:[4EE08B]
00401653 .  C1E0 02     SHL EAX,2
00401656 .  A3 8FE04E00 MOV DWORD PTR DS:[4EE08F],EAX
0040165B .  52          PUSH EDX
0040165C .  6A 00       PUSH 0                              ; /pModule = NULL
0040165E .  E8 DFBC0E00 CALL <JMP.&KERNEL32.GetModuleHandleA> ; \GetModuleH
00401663 .  8BD0        MOV EDX,EAX
--------------------------------------------------------------------------------
```



Borland Delphi 6.0 - 7.0

```
00509CB0 > $   55          PUSH EBP
00509CB1 .   8BEC        MOV EBP,ESP
00509CB3 .   83C4 EC     ADD ESP,-14
00509CB6 .   53          PUSH EBX
00509CB7 .   56          PUSH ESI
00509CB8 .   57          PUSH EDI
00509CB9 .   33C0        XOR EAX,EAX
00509CBB .   8945 EC     MOV DWORD PTR
SS:[EBP-14],EAX
00509CBE .   B8 20975000 MOV
EAX,unpack.00509720
00509CC3 .   E8 84CCEFFF CALL unpack.
0040694C
```

易语言入口

```
00401000 >   E8 06000000     call dump_.0040100B
00401005 50                  push eax
00401006 E8 BB010000     call <jmp.&KERNEL32.ExitProcess>
0040100B 55                  push ebp
0040100C 8BEC                mov ebp,esp
0040100E 81C4 F0FEFFFF add esp,-110
00401014 E9 83000000     jmp dump_.0040109C
00401019 6B72 6E 6C    imul esi,dword ptr ds:[edx+6E],6C
0040101D 6E                  outs dx,byte ptr es:[edi]
```

對於沒有加殼加密或隱藏OEP的軟體,我們可以直接判斷出他用的程式語言

判斷他用什麼程式語言寫得有什麼用呢?

《《《Delphi程序》》》
特征码：FF 93 20 01 00 00 5B C3 53

《《《易语言程序》》》
特征码：FF 55 FC 5F 5E 89 5D F4
特征码来源：krnln.fnr

《《《MFC程序》》》
RELEASE
特征码：FF 55 14 EB 7F FF 75 0C
特征码来源：MFC42.DLL
DEBUG
特征码：FF 55 FC E9 48 04 00 00 33 C9
特征码来源：MFC42D.DLL

使用方法：OD载入程序---F9运行---Alt+M打开内存镜像---Ctrl+B搜索特征码---Ctrl+G跳到找到的地址---F2下断---点击按钮---断下后F7进入CALL（此处即为事件代码）

Q&A