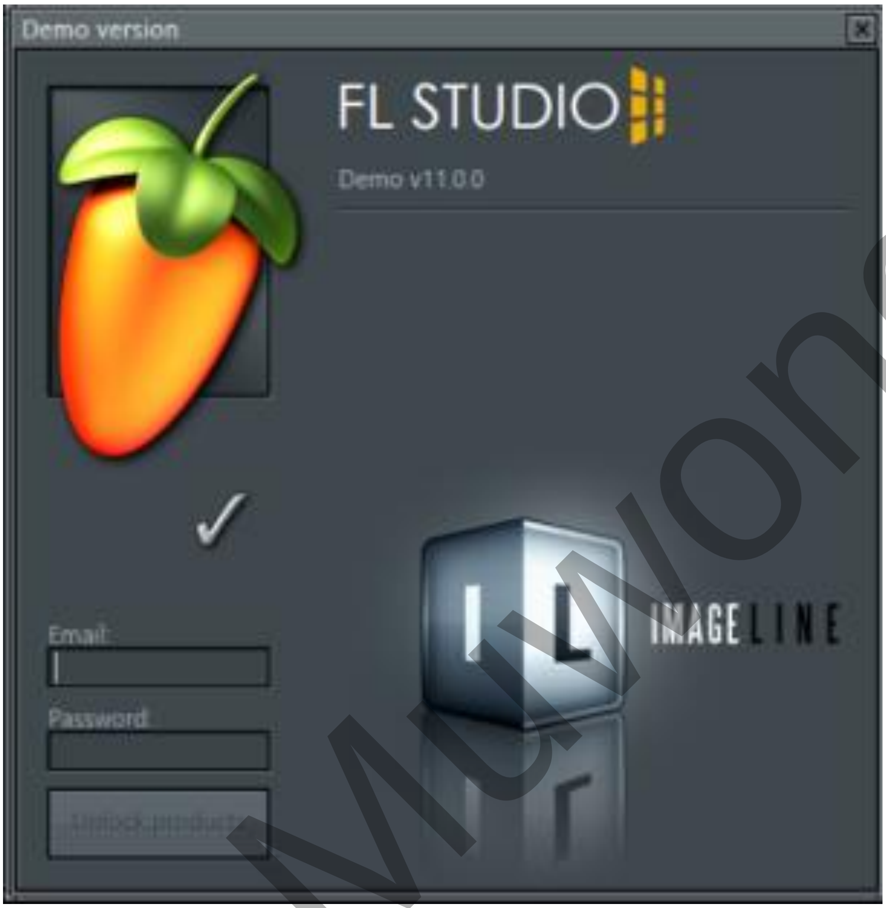
FL STUDIO 11 UNLOCKER REPORT

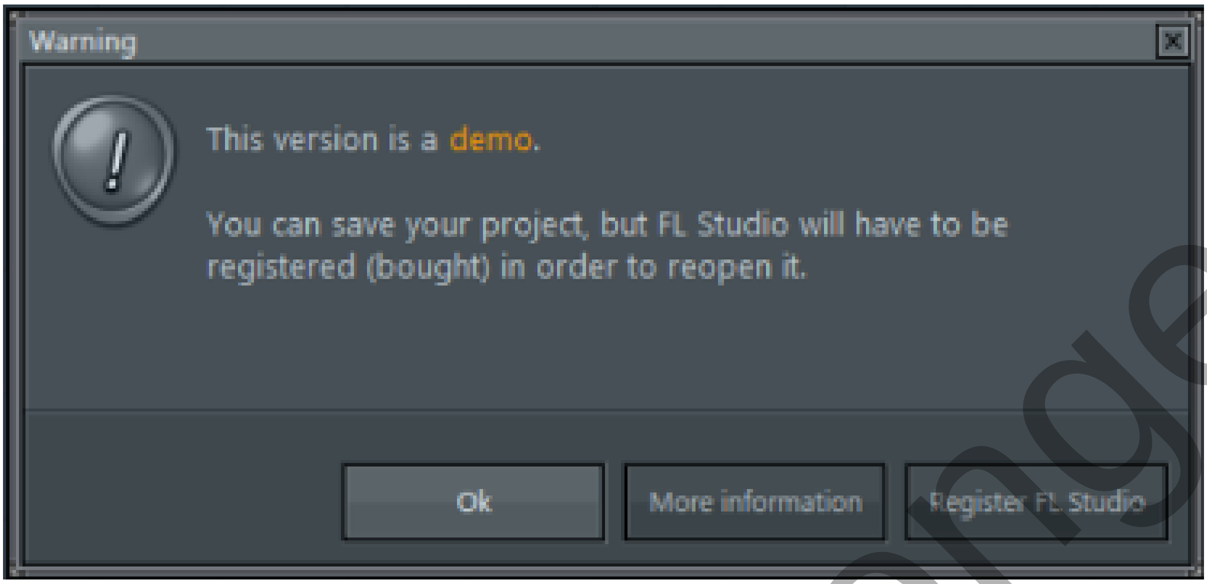
MARK MUWONGE

Unlocking Producer Edition

The Producer Edition is the version of FL Studio 11 with the most features. After installing the software and running the executable (Image-Line\FL Studio 11\FL.exe), the user only has access to the demo version.



This comes with many limitations including the inability to re-open projects once they are saved.



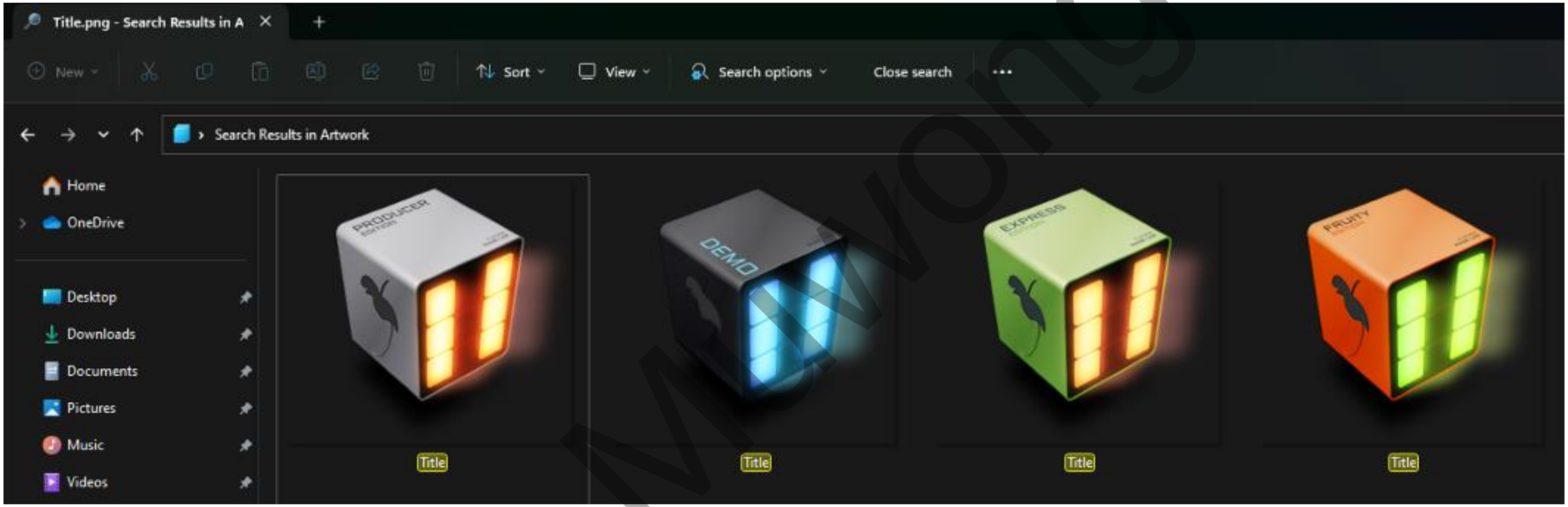
Warning

This version is a demo.

You can save your project, but FL Studio will have to be registered (bought) in order to reopen it.

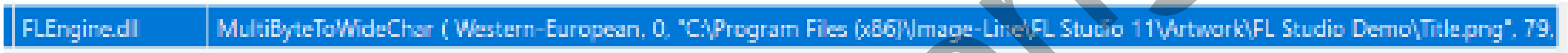
A splash image is displayed when the executable is initially run.

Looking at the directory structure under “Image-Line\FL Studio 11\Artwork” there are several notable directories: FL Studio Demo, FL Studio Express, FL Studio Fruity Edition and FL Studio Producer Edition. These directories all contain a “Title.png” image file. These image files each have their own distinctive appearance.



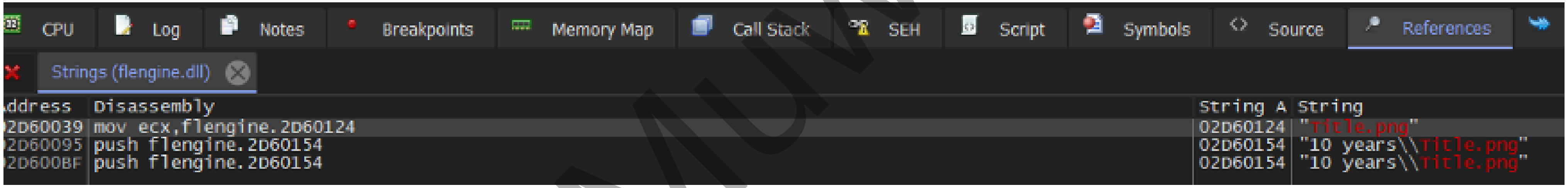
Due to the “Title.png” image file under the “Image-Line\FL Studio 11\Artwork\FL Studio Demo” directory having the same appearance as the start-up splash image and the demo version of the software being loaded, it can be assumed that the FL studio 11 version that gets loaded is dependent on a certain condition and the “Title.png” image file is involved in it.

Using the “Rohitab API monitor” software and monitoring the Windows API calls that FL Studio 11 makes on start-up reveals that the “Title.png” image file is referenced in the “Image-Line\FL Studio 11\FLEngine.dll” module.



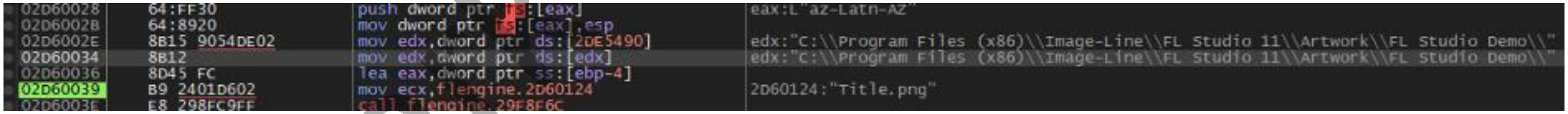
```
FLEngine.dll    MultiByteToWideChar ( Western-European, 0, "C:\Program Files (x86)\Image-Line\FL Studio 11\Artwork\FL Studio Demo\Title.png", 79,
```

Using the “X32dbg” software, setting a breakpoint at the entry point (File offset: 0x3E22C8) to the “FLEngine.dll” module and looking for string references within it containing “Title.png” reveals a “MOV” instruction (File offset: 0x36F439, Arbitrary name: Instruction #1) involving a constant (File offset: 0x36F524) with the value “Title.png”.



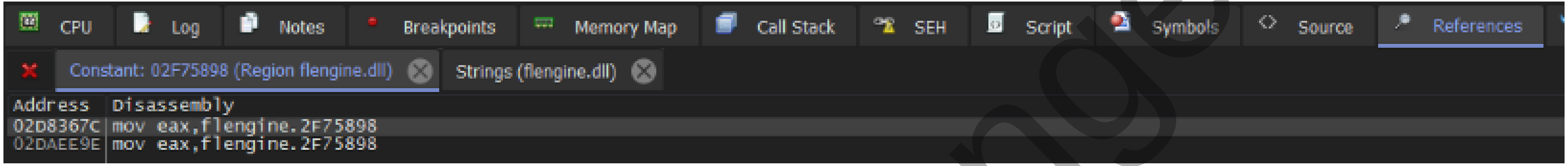
```
ddress   Disassembly                                   String A  String
2D60039  mov ecx,flengine.2D60124                      02D60124  "Title.png"
2D60095  push flengine.2D60154                         02D60154  "10 years\\Title.png"
2D600BF  push flengine.2D60154                         02D60154  "10 years\\Title.png"
```

Upon setting a breakpoint at “Instruction #1”, the EDX register holds an address to a string with the value “Image-Line\FL Studio 11\Artwork\FL Studio Demo”. The EDX register comes to hold the address by getting the value at a hardcoded address (File offset: 0x3F3890, Arbitrary name: Address #1) which is another address (Arbitrary name: Address #2) and getting the value at “Address #2” which is the address of the string.



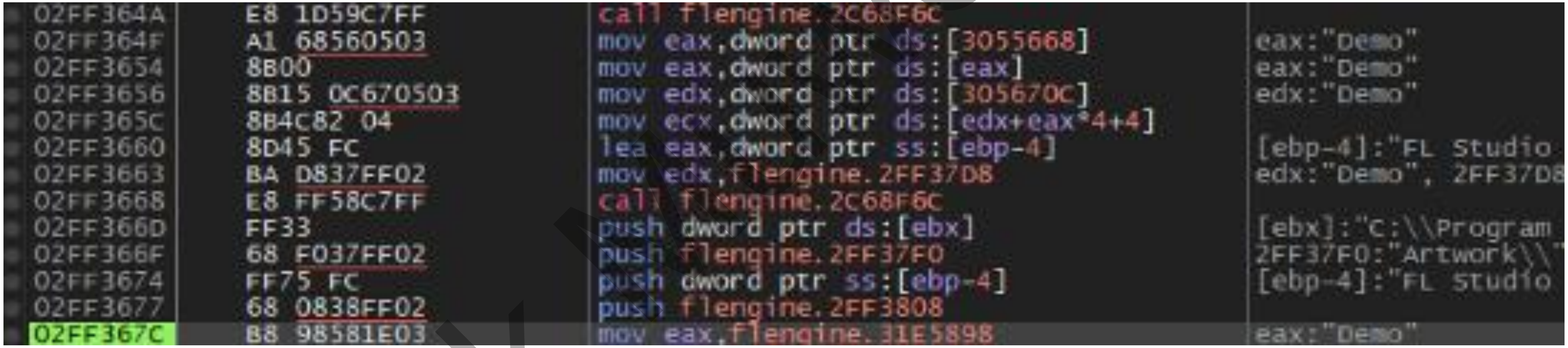
```
02D60028    64:FF30          push dword ptr fs:[eax]                eax:L"az-Latn-AZ"
02D6002B    64:8920          mov dword ptr fs:[eax],esp
02D6002E    8B15 9054DE02    mov edx,dword ptr ds:[2DE5490]         edx:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\Artwork\\FL Studio Demo\\"
02D60034    8B12             mov edx,dword ptr ds:[edx]             edx:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\Artwork\\FL Studio Demo\\"
02D60036    8D45 FC          lea eax,dword ptr ss:[ebp-4]
02D60039    B9 2401D602      mov ecx,flengine.2D60124               2D60124:"Title.png"
02D6003E    E8 298FC9FF      call flengine.29F8F6C
```

Searching references to “Address #2” reveals two instructions.



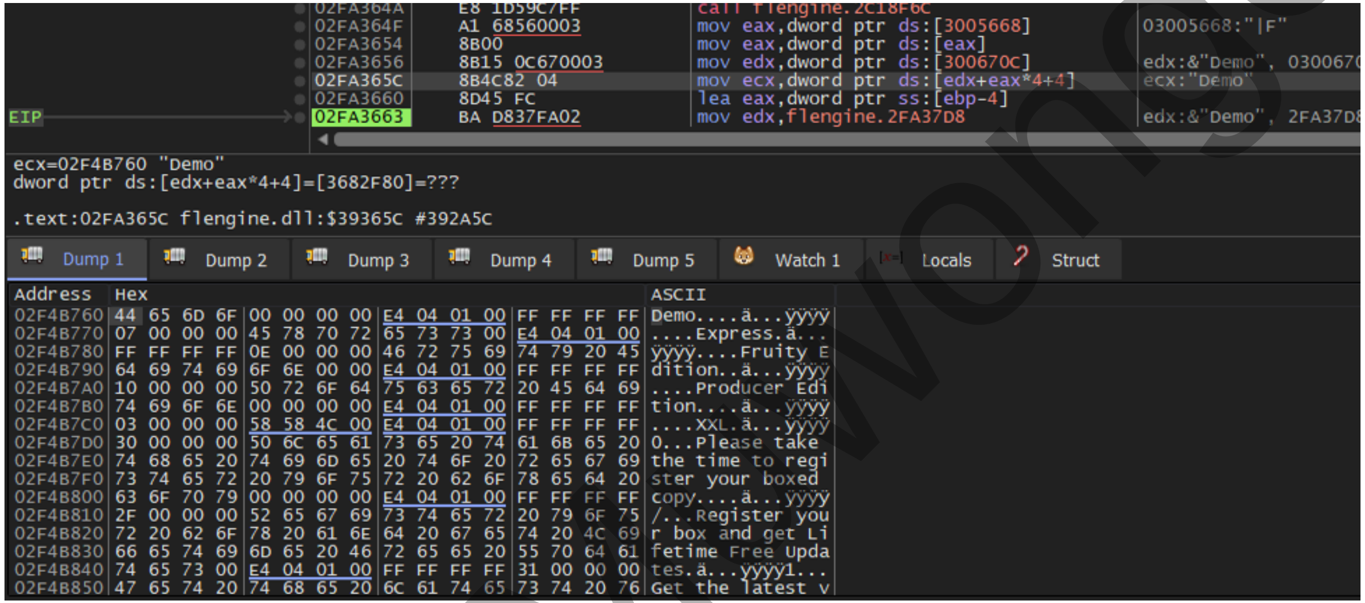
```
Address   Disassembly
02D8367C  mov eax,flengine.2F75898
02DAEE9E  mov eax,flengine.2F75898
```

Restarting FL Studio 11 and setting a breakpoint at the first of the two instructions (File offset: 0x392A7C, Arbitrary name: Instruction #2), both the EAX and EDX register hold addresses to strings with the value “Demo”. A “CALL” instruction appears five instructions before “Instruction #2” that may be responsible for setting the EAX and EDX registers. To be sure, a breakpoint before the “CALL” instruction can be set.



```
02FF364A  E8 1D59C7FF       call flengine.2C68F6C
02FF364F  A1 68560503       mov eax,dword ptr ds:[3055668]      eax:"Demo"
02FF3654  8B00              mov eax,dword ptr ds:[eax]          eax:"Demo"
02FF3656  8B15 0C670503     mov edx,dword ptr ds:[305670C]      edx:"Demo"
02FF365C  8B4C82 04         mov ecx,dword ptr ds:[edx+eax*4+4]
02FF3660  8D45 FC           lea eax,dword ptr ss:[ebp-4]        [ebp-4]:"FL Studio
02FF3663  BA D837FF02       mov edx,flengine.2FF37D8            edx:"Demo", 2FF37D8
02FF3668  E8 FF58C7FF       call flengine.2C68F6C
02FF366D  FF33              push dword ptr ds:[ebx]             [ebx]:"C:\\Program
02FF366F  68 F037FF02       push flengine.2FF37F0               2FF37F0:"Artwork\\"
02FF3674  FF75 FC           push dword ptr ss:[ebp-4]           [ebp-4]:"FL Studio
02FF3677  68 0838FF02       push flengine.2FF3808
02FF367C  B8 98581E03       mov eax,flengine.31E5898            eax:"Demo"
```

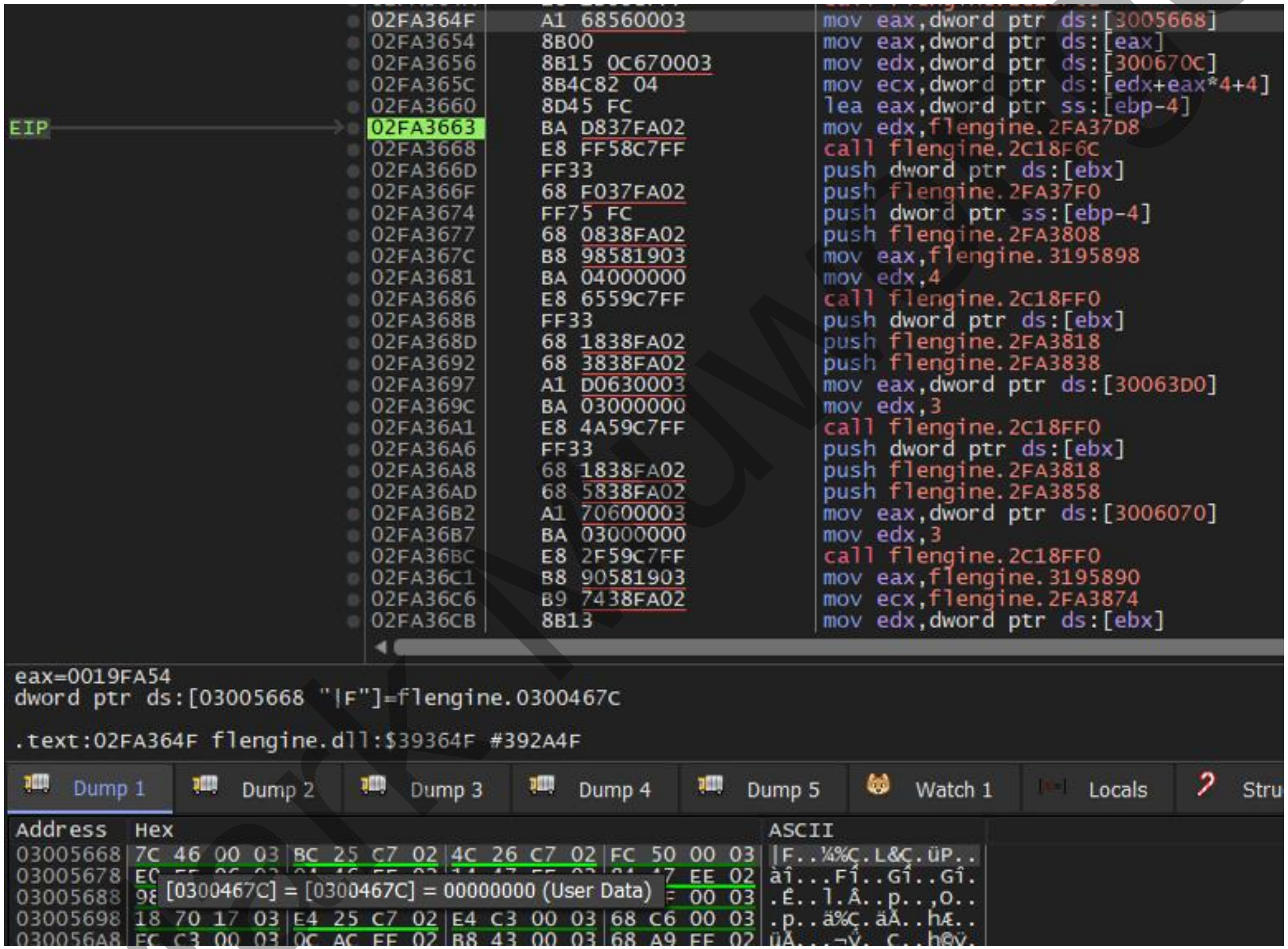
Setting a breakpoint at the instruction before the “CALL” instruction (File offset: 0x392A63, Arbitrary name: Instruction #3) reveals the ECX register holds an address to a string with the value “Demo”. Additionally, a memory dump at the ECX address reveals a list of the FL Studio 11 edition names.



```
                 02FA364A   E8 1D59C7FF      call flengine.2C18F6C
                 02FA364F   A1 68560003      mov eax,dword ptr ds:[3005668]       03005668:"|F"
                 02FA3654   8B00             mov eax,dword ptr ds:[eax]
                 02FA3656   8B15 0C670003    mov edx,dword ptr ds:[300670C]       edx:&"Demo", 0300670
                 02FA365C   8B4C82 04        mov ecx,dword ptr ds:[edx+eax*4+4]   ecx:"Demo"
                 02FA3660   8D45 FC          lea eax,dword ptr ss:[ebp-4]
EIP ------------>02FA3663   BA D837FA02      mov edx,flengine.2FA37D8             edx:&"Demo", 2FA37D8

ecx=02F4B760 "Demo"
dword ptr ds:[edx+eax*4+4]=[3682F80]=???

.text:02FA365C flengine.dll:$39365C #392A5C
```

```
Address   Hex                                               ASCII
02F4B760  44 65 6D 6F 00 00 00 00 E4 04 01 00 FF FF FF FF  Demo....ä...ÿÿÿÿ
02F4B770  07 00 00 00 45 78 70 72 65 73 73 00 E4 04 01 00  ....Express.ä...
02F4B780  FF FF FF FF 0E 00 00 00 46 72 75 69 74 79 20 45  ÿÿÿÿ....Fruity E
02F4B790  64 69 74 69 6F 6E 00 00 E4 04 01 00 FF FF FF FF  dition..ä...ÿÿÿÿ
02F4B7A0  10 00 00 00 50 72 6F 64 75 63 65 72 20 45 64 69  ....Producer Edi
02F4B7B0  74 69 6F 6E 00 00 00 00 E4 04 01 00 FF FF FF FF  tion....ä...ÿÿÿÿ
02F4B7C0  03 00 00 00 58 58 4C 00 E4 04 01 00 FF FF FF FF  ....XXL.ä...ÿÿÿÿ
02F4B7D0  30 00 00 00 50 6C 65 61 73 65 20 74 61 6B 65 20  0...Please take 
02F4B7E0  74 68 65 20 74 69 6D 65 20 74 6F 20 72 65 67 69  the time to regi
02F4B7F0  73 74 65 72 20 79 6F 75 72 20 62 6F 78 65 64 20  ster your boxed 
02F4B800  63 6F 70 79 00 00 00 00 E4 04 01 00 FF FF FF FF  copy....ä...ÿÿÿÿ
02F4B810  2F 00 00 00 52 65 67 69 73 74 65 72 20 79 6F 75  /...Register you
02F4B820  72 20 62 6F 78 20 61 6E 64 20 67 65 74 20 4C 69  r box and get Li
02F4B830  66 65 74 69 6D 65 20 46 72 65 65 20 55 70 64 61  fetime Free Upda
02F4B840  74 65 73 00 E4 04 01 00 FF FF FF FF 31 00 00 00  tes.ä...ÿÿÿÿ1...
02F4B850  47 65 74 20 74 68 65 20 6C 61 74 65 73 74 20 76  Get the latest v
```

Five instructions before "Instruction #3", the EAX register is set with a value at a hardcoded address (File offset: 0x3F3A68, Arbitrary name: Address #3). This value is another address (Arbitrary name: Address #4) that holds the value zero which is stored in EAX.



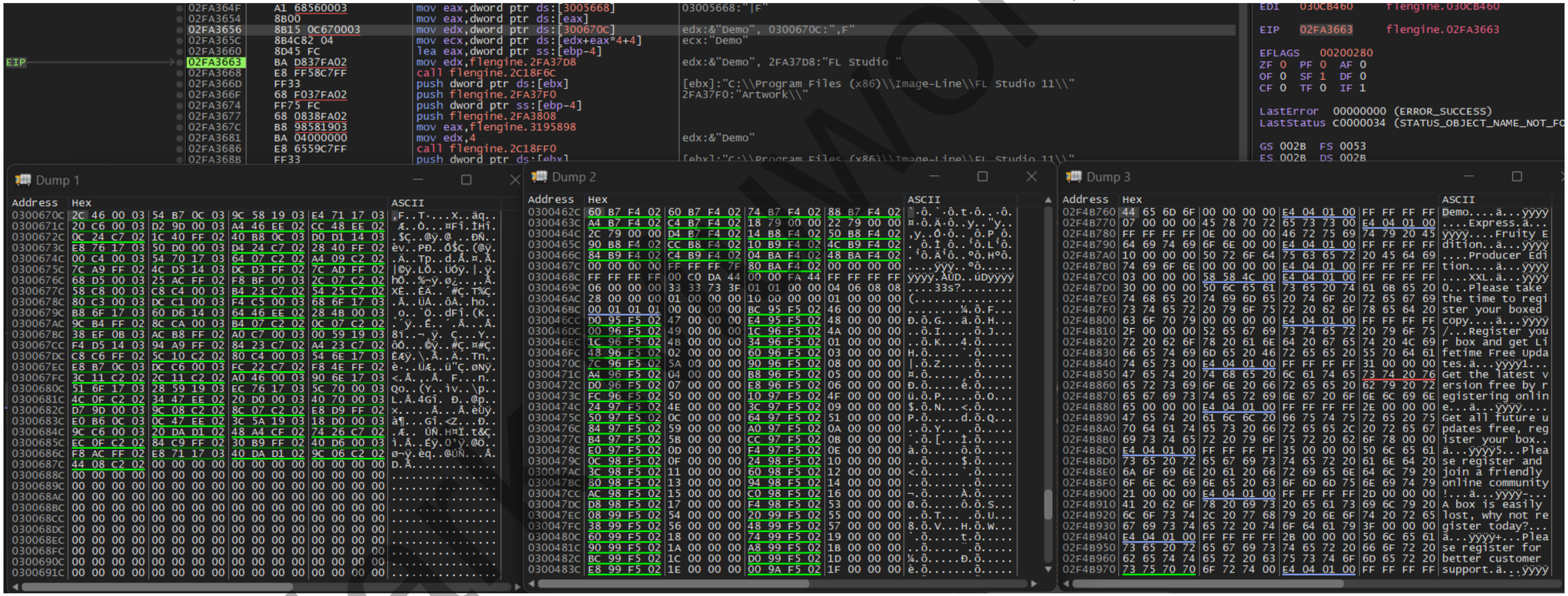
```
     02FA364F   A1 68560003    mov eax,dword ptr ds:[3005668]
     02FA3654   8B00           mov eax,dword ptr ds:[eax]
     02FA3656   8B15 0C670003  mov edx,dword ptr ds:[300670C]
     02FA365C   8B4C82 04      mov ecx,dword ptr ds:[edx+eax*4+4]
     02FA3660   8D45 FC        lea eax,dword ptr ss:[ebp-4]
EIP  02FA3663   BA D837FA02    mov edx,flengine.2FA37D8
     02FA3668   E8 FF58C7FF    call flengine.2C18F6C
     02FA366D   FF33           push dword ptr ds:[ebx]
     02FA366F   68 F037FA02    push flengine.2FA37F0
     02FA3674   FF75 FC        push dword ptr ss:[ebp-4]
     02FA3677   68 0838FA02    push flengine.2FA3808
     02FA367C   B8 98581903    mov eax,flengine.3195898
     02FA3681   BA 04000000    mov edx,4
     02FA3686   E8 6559C7FF    call flengine.2C18FF0
     02FA368B   FF33           push dword ptr ds:[ebx]
     02FA368D   68 1838FA02    push flengine.2FA3818
     02FA3692   68 3838FA02    push flengine.2FA3838
     02FA3697   A1 D0630003    mov eax,dword ptr ds:[30063D0]
     02FA369C   BA 03000000    mov edx,3
     02FA36A1   E8 4A59C7FF    call flengine.2C18FF0
     02FA36A6   FF33           push dword ptr ds:[ebx]
     02FA36A8   68 1838FA02    push flengine.2FA3818
     02FA36AD   68 5838FA02    push flengine.2FA3858
     02FA36B2   A1 70600003    mov eax,dword ptr ds:[3006070]
     02FA36B7   BA 03000000    mov edx,3
     02FA36BC   E8 2F59C7FF    call flengine.2C18FF0
     02FA36C1   B8 90581903    mov eax,flengine.3195890
     02FA36C6   B9 7438FA02    mov ecx,flengine.2FA3874
     02FA36CB   8B13           mov edx,dword ptr ds:[ebx]

eax=0019FA54
dword ptr ds:[03005668 "|F"]=flengine.0300467C

.text:02FA364F flengine.dll:$39364F #392A4F
```

```
Address   Hex                                              ASCII
03005668  7C 46 00 03 BC 25 C7 02 4C 26 C7 02 FC 50 00 03  |F..¼%Ç.L&Ç.üP..
03005678  EC                                   7 EE 02  àî...Fî..Gî..Gî.
03005688  98                                   F 00 03  .Ê..l.Â..p..,o..
03005698  18 70 17 03 E4 25 C7 02 E4 C3 00 03 68 C6 00 03  .p..ä%Ç.äÃ..hÆ..
030056A8  FC C3 00 03 0C AC EE 02 B8 43 00 03 68 A9 EE 02  üÃ...¬ý. C..h©ÿ.
```

[0300467C] = [0300467C] = 00000000 (User Data)

Three instructions before “Instruction #3” the EDX register is set with the value of a hardcoded address (Arbitrary name: Address #5). The value at “Address #5” is another address that points to the first character of the string value “Demo” (“D”).

Two instructions before “Instruction #3” (File offset: 0x392A5C, Arbitrary name: Instruction #4) shows the ECX register being set. The address that comes from the dereferenced EDX register is used as a base and the numeric value that comes from the dereferenced EAX register is used as an offset to each of the FL Studio 11 edition names. When the EAX register is zero, the ECX register holds the address of the first character of the string value “Demo” (“D”). When the EAX register is one, the ECX register holds the address of the first character of the string value “Express” (“E”) etc.



```
     02FA364F  A1 68560003    mov eax,dword ptr ds:[3005668]        03005668:"|F"
     02FA3654  8B00           mov eax,dword ptr ds:[eax]
     02FA3656  8B15 0C670003  mov edx,dword ptr ds:[300670C]        edx:&"Demo", 0300670C:",F"
     02FA365C  8B4C82 04      mov ecx,dword ptr ds:[edx+eax*4+4]    ecx:"Demo"
     02FA3660  8D45 FC        lea eax,dword ptr ss:[ebp-4]
EIP  02FA3663  BA D837FA02    mov edx,flengine.2FA37D8              edx:&"Demo", 2FA37D8:"FL Studio "
     02FA3668  E8 FF58C7FF    call flengine.2C18F6C
     02FA366D  FF33           push dword ptr ds:[ebx]               [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
     02FA366F  68 F037FA02    push flengine.2FA37F0                 2FA37F0:"Artwork\\"
     02FA3674  FF75 FC        push dword ptr ss:[ebp-4]
     02FA3677  68 0838FA02    push flengine.2FA3808
     02FA367C  B8 98581903    mov eax,flengine.3195898
     02FA3681  BA 04000000    mov edx,4                             edx:&"Demo"
     02FA3686  E8 6559C7FF    call flengine.2C18FF0
     02FA368B  FF33           push dword ptr ds:[ebx]               [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
```

```
EDI  030CB460   flengine.030CB460

EIP  02FA3663   flengine.02FA3663

EFLAGS  00200280
ZF 0  PF 0  AF 0
OF 0  SF 1  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FO

GS 002B  FS 0053
ES 002B  DS 002B
```

Dump 1

```
Address   Hex                                              ASCII
0300670C  2C 46 00 03 54 B7 0C 03 9C 58 19 03 E4 71 17 03  ,F..T·...X..äq..
0300671C  20 C6 00 03 D2 9D 00 03 A4 46 EE 02 CC 48 EE 02   Æ..Ò...¤Fî.ÌHî.
0300672C  0C 24 C7 02 1C 40 FF 02 40 B8 0C 03 D0 D1 14 03  .$Ç..@ÿ.@...ÐÑ..
0300673C  E8 76 17 03 50 D0 00 03 D4 24 C7 02 28 40 FF 02  èv..PÐ..Ô$Ç.(@ÿ.
0300674C  00 C4 00 03 54 70 17 03 64 07 C2 02 A4 09 C2 02  .Ä..Tp..d.Â.¤.Â.
0300675C  7C A9 FF 02 4C D5 14 03 DC D3 FF 02 7C AD FF 02  |©ÿ.LÕ..ÜÓÿ.|.ÿ.
0300676C  68 D5 00 03 25 AC FF 02 F8 BF 00 03 2C 07 C2 02  hÕ..%¬ÿ.ø¿..,.Â.
0300677C  58 C8 00 03 C8 C4 00 03 B4 23 C7 02 54 25 C7 02  XÈ..ÈÄ..´#Ç.T%Ç.
0300678C  80 C3 00 03 DC C1 00 03 F4 C5 00 03 68 6F 17 03  .Ã..ÜÁ..ôÅ..ho..
0300679C  B8 6F 17 03 60 D6 14 03 64 46 EE 02 28 4B 00 03  ¸o..`Ö..dFî.(K..
030067AC  9C B4 FF 02 8C CA 00 03 B4 07 C2 02 0C 07 C2 02  .´ÿ..Ê..´.Â...Â.
030067BC  38 EF 0B 03 AC B8 FF 02 A0 C7 00 03 00 59 19 03  8ï..¬¸ÿ. Ç...Y..
030067CC  F4 D5 14 03 94 A9 FF 02 84 23 C7 02 A4 23 C7 02  ôÕ...©ÿ..#Ç.¤#Ç.
030067DC  C8 C6 FF 02 5C 10 C2 02 80 C4 00 03 54 6E 17 03  ÈÆÿ.\.Â..Ä..Tn..
030067EC  E8 B7 0C 03 DC C6 00 03 FC 22 C7 02 F8 4E FF 02  è·..ÜÆ..ü"Ç.øNÿ.
030067FC  3C 11 C2 02 2C 11 C2 02 A0 46 00 03 90 6E 17 03  <.Â.,.Â. F...n..
0300680C  51 6F 17 03 28 59 19 03 EC 76 17 03 5C 70 00 03  Qo..(Y..ìv..\p..
0300681C  4C 0F C2 02 34 47 EE 02 20 D0 00 03 40 70 00 03  L.Â.4Gî. Ð..@p..
0300682C  D7 9D 00 03 9C 08 C2 02 8C 07 C2 02 E8 D9 FF 02  ×.....Â...Â.èÙÿ.
0300683C  E0 B6 0C 03 0C 47 EE 02 3C 5A 19 03 18 D0 00 03  à¶...Gî.<Z...Ð..
0300684C  9C C6 00 03 20 DA D1 02 48 A4 CF 02 74 26 C7 02  .Æ.. ÚÑ.H¤Ï.t&Ç.
0300685C  EC 0F C2 02 84 C9 FF 02 30 B9 FF 02 40 D6 00 03  ì.Â..Éÿ.0¹ÿ.@Ö..
0300686C  F8 AC FF 02 E8 71 17 03 40 DA D1 02 9C 06 C2 02  ø¬ÿ.èq..@ÚÑ...Â.
0300687C  44 08 C2 02 00 00 00 00 00 00 00 00 00 00 00 00  D.Â.............
0300688C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0300689C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068DC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
030068FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0300690C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0300691C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

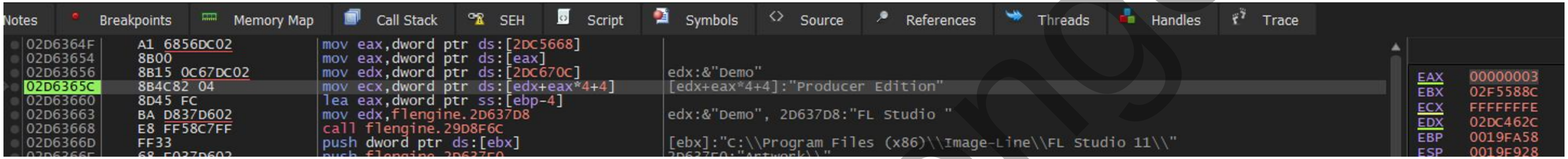
Dump 2

```
Address   Hex                                              ASCII
0300462C  60 B7 F4 02 60 B7 F4 02 74 B7 F4 02 88 B7 F4 02  `·ô.`·ô.t·ô..·ô.
0300463C  A4 B7 F4 02 C4 B7 F4 02 18 79 00 00 22 79 00 00  ¤·ô.Ä·ô..y.."y..
0300464C  2C 79 00 00 D4 B7 F4 02 14 B8 F4 02 50 B8 F4 02  ,y..Ô·ô..¸ô.P¸ô.
0300465C  90 B8 F4 02 CC B8 F4 02 10 B9 F4 02 4C B9 F4 02  .¸ô.Ì¸ô..¹ô.L¹ô.
0300466C  84 B9 F4 02 C4 B9 F4 02 04 BA F4 02 48 BA F4 02  .¹ô.Ä¹ô..ºô.Hºô.
0300467C  00 00 00 00 FF FF FF 7F 80 BA F4 02 00 00 00 00  ....ÿÿÿ..ºô.....
0300468C  FF FF FF FF 00 C0 DA 44 00 00 FA 44 FF FF FF FF  ÿÿÿÿ.ÀÚD..úDÿÿÿÿ
0300469C  06 00 00 00 33 33 73 3F 01 01 00 00 04 06 08 08  ....33s?........
030046AC  28 00 00 00 01 00 00 00 10 00 00 00 01 00 00 00  (...............
030046BC  00 01 01 01 00 00 00 00 BC 95 F5 02 46 00 00 00  ........¼.õ.F...
030046CC  D0 95 F5 02 47 00 00 00 E4 95 F5 02 48 00 00 00  Ð.õ.G...ä.õ.H...
030046DC  00 96 F5 02 49 00 00 00 1C 96 F5 02 4A 00 00 00  ..õ.I.....õ.J...
030046EC  1C 96 F5 02 4B 00 00 00 34 96 F5 02 01 00 00 00  ..õ.K...4.õ.....
030046FC  48 96 F5 02 02 00 00 00 60 96 F5 02 03 00 00 00  H.õ.....`.õ.....
0300470C  7C 96 F5 02 5A 00 00 00 90 96 F5 02 08 00 00 00  |.õ.Z.....õ.....
0300471C  A4 96 F5 02 04 00 00 00 B8 96 F5 02 05 00 00 00  ¤.õ.....¸.õ.....
0300472C  D0 96 F5 02 07 00 00 00 E8 96 F5 02 06 00 00 00  Ð.õ.....è.õ.....
0300473C  FC 96 F5 02 50 00 00 00 10 97 F5 02 4F 00 00 00  ü.õ.P.....õ.O...
0300474C  24 97 F5 02 4E 00 00 00 3C 97 F5 02 09 00 00 00  $.õ.N...<.õ.....
0300475C  50 97 F5 02 0C 00 00 00 64 97 F5 02 51 00 00 00  P.õ.....d.õ.Q...
0300476C  84 97 F5 02 59 00 00 00 A0 97 F5 02 0A 00 00 00  ..õ.Y... .õ.....
0300477C  B4 97 F5 02 5B 00 00 00 CC 97 F5 02 0B 00 00 00  ´.õ.[...Ì.õ.....
0300478C  E0 97 F5 02 0D 00 00 00 F4 97 F5 02 0E 00 00 00  à.õ.....ô.õ.....
0300479C  0C 98 F5 02 0F 00 00 00 24 98 F5 02 10 00 00 00  ..õ.....$.õ.....
030047AC  3C 98 F5 02 11 00 00 00 60 98 F5 02 12 00 00 00  <.õ.....`.õ.....
030047BC  80 98 F5 02 13 00 00 00 94 98 F5 02 14 00 00 00  ..õ.......õ.....
030047CC  AC 98 F5 02 15 00 00 00 C0 98 F5 02 16 00 00 00  ¬.õ.....À.õ.....
030047DC  D8 98 F5 02 17 00 00 00 F4 98 F5 02 53 00 00 00  Ø.õ.....ô.õ.S...
030047EC  08 99 F5 02 54 00 00 00 20 99 F5 02 55 00 00 00  ..õ.T... .õ.U...
030047FC  38 99 F5 02 56 00 00 00 48 99 F5 02 57 00 00 00  8.õ.V...H.õ.W...
0300480C  60 99 F5 02 18 00 00 00 74 99 F5 02 19 00 00 00  `.õ.....t.õ.....
0300481C  90 99 F5 02 1A 00 00 00 A8 99 F5 02 1B 00 00 00  ..õ.....¨.õ.....
0300482C  BC 99 F5 02 1C 00 00 00 D0 99 F5 02 1D 00 00 00  ¼.õ.....Ð.õ.....
0300483C  E8 99 F5 02 1E 00 00 00 00 9A F5 02 1F 00 00 00  è.õ.......õ.....
```

Dump 3

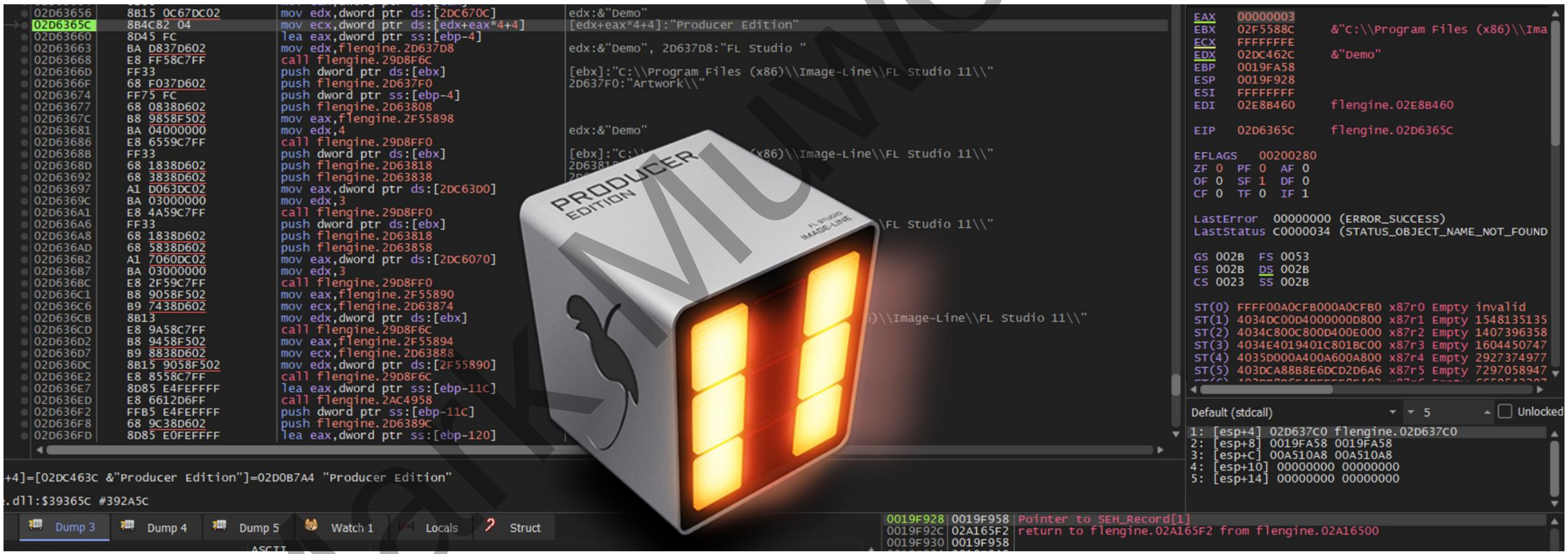
```
Address   Hex                                              ASCII
02F4B760  44 65 6D 6F 00 00 00 00 E4 04 01 00 FF FF FF FF  Demo....ä...ÿÿÿÿ
02F4B770  07 00 00 00 45 78 70 72 65 73 73 00 E4 04 01 00  ....Express.ä...
02F4B780  FF FF FF FF 0E 00 00 00 46 72 75 69 74 79 20 45  ÿÿÿÿ....Fruity E
02F4B790  64 69 74 69 6F 6E 00 00 E4 04 01 00 FF FF FF FF  dition..ä...ÿÿÿÿ
02F4B7A0  10 00 00 00 50 72 6F 64 75 63 65 72 20 45 64 69  ....Producer Edi
02F4B7B0  74 69 6F 6E 00 00 00 00 E4 04 01 00 FF FF FF FF  tion....ä...ÿÿÿÿ
02F4B7C0  03 00 00 00 58 58 4C 00 E4 04 01 00 FF FF FF FF  ....XXL.ä...ÿÿÿÿ
02F4B7D0  30 00 00 00 50 6C 65 61 73 65 20 74 61 6B 65 20  0...Please take 
02F4B7E0  74 68 65 20 74 69 6D 65 20 74 6F 20 72 65 67 69  the time to regi
02F4B7F0  73 74 65 72 20 79 6F 75 72 20 62 6F 78 65 64 20  ster your boxed 
02F4B800  63 6F 70 79 00 00 00 00 E4 04 01 00 FF FF FF FF  copy....ä...ÿÿÿÿ
02F4B810  2F 00 00 00 52 65 67 69 73 74 65 72 20 79 6F 75  /...Register you
02F4B820  72 20 62 6F 78 20 61 6E 64 20 67 65 74 20 4C 69  r box and get Li
02F4B830  66 65 74 69 6D 65 20 46 72 65 65 20 55 70 64 61  fetime Free Upda
02F4B840  74 65 73 00 E4 04 01 00 FF FF FF FF 31 00 00 00  tes.ä...ÿÿÿÿ1...
02F4B850  47 65 74 20 74 68 65 20 6C 61 74 65 73 74 20 76  Get the latest v
02F4B860  65 72 73 69 6F 6E 20 66 72 65 65 20 62 79 20 72  ersion free by r
02F4B870  65 67 69 73 74 65 72 69 6E 67 20 6F 6E 6C 69 6E  egistering onlin
02F4B880  65 00 00 00 E4 04 01 00 FF FF FF FF 2E 00 00 00  e...ä...ÿÿÿÿ....
02F4B890  47 65 74 20 61 6C 6C 20 66 75 74 75 72 65 20 75  Get all future u
02F4B8A0  70 64 61 74 65 73 20 66 72 65 65 2C 20 72 65 67  pdates free, reg
02F4B8B0  69 73 74 65 72 20 79 6F 75 72 20 62 6F 78 00 00  ister your box..
02F4B8C0  E4 04 01 00 FF FF FF FF 35 00 00 00 50 6C 65 61  ä...ÿÿÿÿ5...Plea
02F4B8D0  73 65 20 72 65 67 69 73 74 65 72 20 61 6E 64 20  se register and 
02F4B8E0  6A 6F 69 6E 20 61 20 66 72 69 65 6E 64 6C 79 20  join a friendly 
02F4B8F0  6F 6E 6C 69 6E 65 20 63 6F 6D 6D 75 6E 69 74 79  online community
02F4B900  21 00 00 00 E4 04 01 00 FF FF FF FF 2D 00 00 00  !...ä...ÿÿÿÿ-...
02F4B910  41 20 62 6F 78 20 69 73 20 65 61 73 69 6C 79 20  A box is easily 
02F4B920  6C 6F 73 74 2C 20 77 68 79 20 6E 6F 74 20 72 65  lost, why not re
02F4B930  67 69 73 74 65 72 20 74 6F 64 61 79 3F 00 00 00  gister today?...
02F4B940  E4 04 01 00 FF FF FF FF 2B 00 00 00 50 6C 65 61  ä...ÿÿÿÿ+...Plea
02F4B950  73 65 20 72 65 67 69 73 74 65 72 20 66 6F 72 20  se register for 
02F4B960  62 65 74 74 65 72 20 63 75 73 74 6F 6D 65 72 20  better customer 
02F4B970  73 75 70 70 6F 72 74 00 E4 04 01 00 FF FF FF FF  support.ä...ÿÿÿÿ
```

From here it can be assumed that restarting FL Studio 11, making a breakpoint at “Instruction #4”, changing the EAX register value to three and resuming the application will cause the “Producer Edition” splash image to appear on start-up.



```
02D6364F    A1 6856DC02      mov eax,dword ptr ds:[2DC5668]
02D63654    8B00             mov eax,dword ptr ds:[eax]
02D63656    8B15 0C67DC02    mov edx,dword ptr ds:[2DC670C]       edx:&"Demo"
02D6365C    8B4C82 04        mov ecx,dword ptr ds:[edx+eax*4+4]   [edx+eax*4+4]:"Producer Edition"
02D63660    8D45 FC          lea eax,dword ptr ss:[ebp-4]
02D63663    BA D837D602      mov edx,flengine.2D637D8             edx:&"Demo", 2D637D8:"FL Studio "
02D63668    E8 FF58C7FF      call flengine.29D8F6C
02D6366D    FF33             push dword ptr ds:[ebx]              [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
02D6366F    68 F037D602      push flengine.2D637F0                2D637F0:"Artwork\\"

EAX  00000003
EBX  02F5588C
ECX  FFFFFFFE
EDX  02DC462C
EBP  0019FA58
ESP  0019F928
```

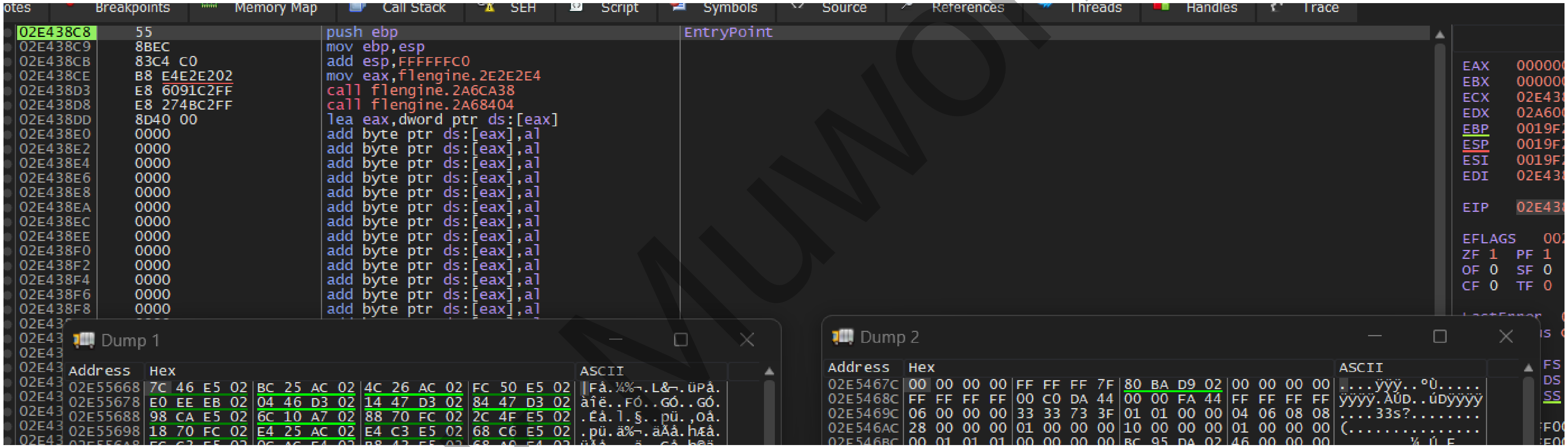
This is precisely what happens.



```
02D63656    8B15 0C67DC02    mov edx,dword ptr ds:[2DC670C]       edx:&"Demo"
02D6365C    8B4C82 04        mov ecx,dword ptr ds:[edx+eax*4+4]   [edx+eax*4+4]:"Producer Edition"
02D63660    8D45 FC          lea eax,dword ptr ss:[ebp-4]
02D63663    BA D837D602      mov edx,flengine.2D637D8             edx:&"Demo", 2D637D8:"FL Studio "
02D63668    E8 FF58C7FF      call flengine.29D8F6C
02D6366D    FF33             push dword ptr ds:[ebx]              [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
02D6366F    68 F037D602      push flengine.2D637F0                2D637F0:"Artwork\\"
02D63674    FF75 FC          push dword ptr ss:[ebp-4]
02D63677    68 0838D602      push flengine.2D63808
02D6367C    B8 9858F502      mov eax,flengine.2F55898
02D63681    BA 04000000      mov edx,4                            edx:&"Demo"
02D63686    E8 6559C7FF      call flengine.29D8FF0
02D6368B    FF33             push dword ptr ds:[ebx]              [ebx]:"C:\\                (x86)\\Image-Line\\FL Studio 11\\"
02D6368D    68 1838D602      push flengine.2D63818                2D6381
02D63692    68 3838D602      push flengine.2D63838
02D63697    A1 D063DC02      mov eax,dword ptr ds:[2DC63D0]
02D6369C    BA 03000000      mov edx,3
02D636A1    E8 4A59C7FF      call flengine.29D8FF0
02D636A6    FF33             push dword ptr ds:[ebx]                                  FL Studio 11\\"
02D636A8    68 1838D602      push flengine.2D63818
02D636AD    68 5838D602      push flengine.2D63858
02D636B2    A1 7060DC02      mov eax,dword ptr ds:[2DC6070]
02D636B7    BA 03000000      mov edx,3
02D636BC    E8 2F59C7FF      call flengine.29D8FF0
02D636C1    B8 9058F502      mov eax,flengine.2F55890
02D636C6    B9 7438D602      mov ecx,flengine.2D63874
02D636CB    8B13             mov edx,dword ptr ds:[ebx]                               )\\Image-Line\\FL Studio 11\\"
02D636CD    E8 9A58C7FF      call flengine.29D8F6C
02D636D2    B8 9458F502      mov eax,flengine.2F55894
02D636D7    B9 8838D602      mov ecx,flengine.2D63888
02D636DC    8B15 9058F502    mov edx,dword ptr ds:[2F55890]
02D636E2    E8 8558C7FF      call flengine.29D8F6C
02D636E7    8D85 E4FEFFFF    lea eax,dword ptr ss:[ebp-11C]
02D636ED    E8 6612D6FF      call flengine.2AC4958
02D636F2    FFB5 E4FEFFFF    push dword ptr ss:[ebp-11C]
02D636F8    68 9C38D602      push flengine.2D6389C
02D636FD    8D85 E0FEFFFF    lea eax,dword ptr ss:[ebp-120]

+4]=[02DC463C &"Producer Edition"]=02D0B7A4 "Producer Edition"

.dll:$39365C #392A5C

EAX     00000003
EBX     02F5588C     &"C:\\Program Files (x86)\\Ima
ECX     FFFFFFFE
EDX     02DC462C     &"Demo"
EBP     0019FA58
ESP     0019F928
ESI     FFFFFFFF
EDI     02E8B460     flengine.02E8B460

EIP     02D6365C     flengine.02D6365C

EFLAGS    00200280
ZF 0  PF 0  AF 0
OF 0  SF 1  DF 0
CF 0  TF 0  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C0000034 (STATUS_OBJECT_NAME_NOT_FOUND

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) FFFF00A0CFB000A0CFB0 x87r0 Empty invalid
ST(1) 4034DC00D4000000D800 x87r1 Empty 1548135135
ST(2) 4034C800C800D400E000 x87r2 Empty 1407396358
ST(3) 4034E4019401C801BC00 x87r3 Empty 1604450747
ST(4) 4035D000A400A600A800 x87r4 Empty 2927374977
ST(5) 403DCA88B8E6DCD2D6A6 x87r5 Empty 7297058947

1: [esp+4]  02D637C0 flengine.02D637C0
2: [esp+8]  0019FA58 0019FA58
3: [esp+C]  00A510A8 00A510A8
4: [esp+10] 00000000 00000000
5: [esp+14] 00000000 00000000

0019F928 0019F958 Pointer to SEH_Record[1]
0019F92C 02A165F2 return to flengine.02A165F2 from flengine.02A16500
0019F930 0019F958
```

However as expected, the application is still the demo version. What can be deduced is that the numerical value at address “Address #4” is used to determine which splash image is presented and perhaps the loaded version. The reason the demo version was loaded could be due to the splash image selection sequence occurring after the version selection sequence occurs.

Restarting FL Studio 11 and setting a breakpoint at the entry point of FLEngine.dll, reveals that “Address #4” holds the value of zero by default. Therefore during the version selection sequence, it can be assumed that there would be no need to explicitly set the value at “Address #4” to zero after determining that the demo version should run.



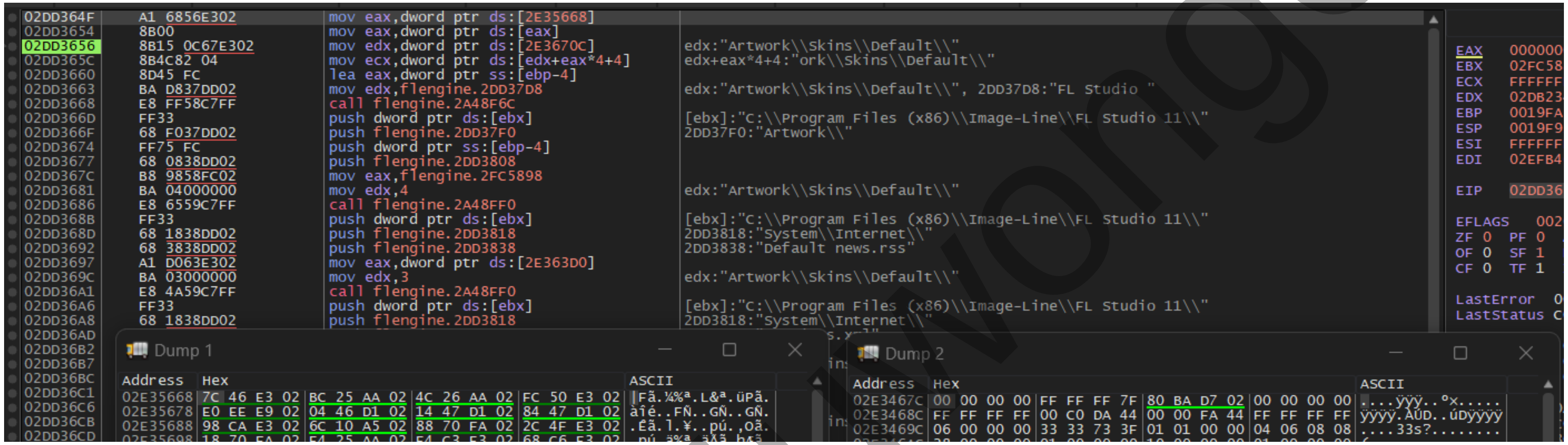
```
02E438C8   55          push ebp                            EntryPoint
02E438C9   8BEC        mov ebp,esp
02E438CB   83C4 C0     add esp,FFFFFFC0
02E438CE   B8 E4E2E202 mov eax,flengine.2E2E2E4
02E438D3   E8 6091C2FF call flengine.2A6CA38
02E438D8   E8 274BC2FF call flengine.2A68404
02E438DD   8D40 00     lea eax,dword ptr ds:[eax]
02E438E0   0000        add byte ptr ds:[eax],al
02E438E2   0000        add byte ptr ds:[eax],al
02E438E4   0000        add byte ptr ds:[eax],al
02E438E6   0000        add byte ptr ds:[eax],al
02E438E8   0000        add byte ptr ds:[eax],al
02E438EA   0000        add byte ptr ds:[eax],al
02E438EC   0000        add byte ptr ds:[eax],al
02E438EE   0000        add byte ptr ds:[eax],al
02E438F0   0000        add byte ptr ds:[eax],al
02E438F2   0000        add byte ptr ds:[eax],al
02E438F4   0000        add byte ptr ds:[eax],al
02E438F6   0000        add byte ptr ds:[eax],al
02E438F8   0000        add byte ptr ds:[eax],al
```

```
EAX     00000
EBX     00000
ECX     02E43
EDX     02A60
EBP     0019F
ESP     0019F
ESI     0019F
EDI     02E43

EIP     02E43

EFLAGS  002
ZF 1  PF 1
OF 0  SF 0
CF 0  TF 0
```

```
Dump 1
Address   Hex                                                  ASCII
02E55668  7C 46 E5 02 BC 25 AC 02 4C 26 AC 02 FC 50 E5 02  |Få.¼%¬.L&¬.üPå.
02E55678  E0 EE EB 02 04 46 D3 02 14 47 D3 02 84 47 D3 02  àîë..FÓ..GÓ..GÓ.
02E55688  98 CA E5 02 6C 10 A7 02 88 70 FC 02 2C 4F E5 02  .Êå.l.§..pü.,Oå.
02E55698  18 70 FC 02 E4 25 AC 02 E4 C3 E5 02 68 C6 E5 02  .pü.ä%¬.äÃå.hÆå.
```

```
Dump 2
Address   Hex                                                  ASCII
02E5467C  00 00 00 00 FF FF FF 7F 80 BA D9 02 00 00 00 00  ....ÿÿÿ..ºÙ.....
02E5468C  FF FF FF FF 00 C0 DA 44 00 00 FA 44 FF FF FF FF  ÿÿÿÿ.ÀÚD..úDÿÿÿÿ
02E5469C  06 00 00 00 33 33 73 3F 01 01 00 00 04 06 08 08  ....33s?........
02E546AC  28 00 00 00 01 00 00 00 10 00 00 00 01 00 00 00  (...............
```

This assumption proves to be true when setting a hardware breakpoint at “Address #4”. The breakpoint gets triggered twice and at no point is “Address #4” written to.

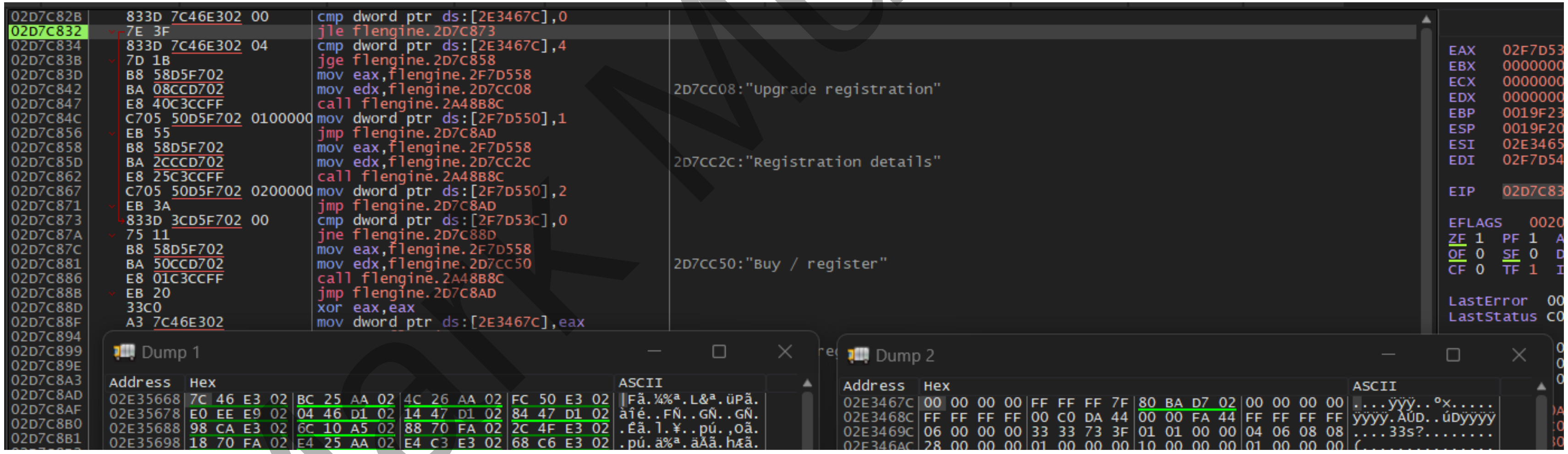


```
02DD364F   A1 6856E302        mov eax,dword ptr ds:[2E35668]
02DD3654   8B00               mov eax,dword ptr ds:[eax]
02DD3656   8B15 0C67E302      mov edx,dword ptr ds:[2E3670C]          edx:"Artwork\\Skins\\Default\\"
02DD365C   8B4C82 04          mov ecx,dword ptr ds:[edx+eax*4+4]      edx+eax*4+4:"ork\\Skins\\Default\\"
02DD3660   8D45 FC            lea eax,dword ptr ss:[ebp-4]
02DD3663   BA D837DD02        mov edx,flengine.2DD37D8                edx:"Artwork\\Skins\\Default\\", 2DD37D8:"FL Studio "
02DD3668   E8 FF58C7FF        call flengine.2A48F6C
02DD366D   FF33               push dword ptr ds:[ebx]                 [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
02DD366F   68 F037DD02        push flengine.2DD37F0                   2DD37F0:"Artwork\\"
02DD3674   FF75 FC            push dword ptr ss:[ebp-4]
02DD3677   68 0838DD02        push flengine.2DD3808
02DD367C   B8 9858FC02        mov eax,flengine.2FC5898
02DD3681   BA 04000000        mov edx,4                               edx:"Artwork\\Skins\\Default\\"
02DD3686   E8 6559C7FF        call flengine.2A48FF0
02DD368B   FF33               push dword ptr ds:[ebx]                 [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
02DD368D   68 1838DD02        push flengine.2DD3818                   2DD3818:"System\\Internet\\"
02DD3692   68 3838DD02        push flengine.2DD3838                   2DD3838:"Default news.rss"
02DD3697   A1 D063E302        mov eax,dword ptr ds:[2E363D0]
02DD369C   BA 03000000        mov edx,3                               edx:"Artwork\\Skins\\Default\\"
02DD36A1   E8 4A59C7FF        call flengine.2A48FF0
02DD36A6   FF33               push dword ptr ds:[ebx]                 [ebx]:"C:\\Program Files (x86)\\Image-Line\\FL Studio 11\\"
02DD36A8   68 1838DD02        push flengine.2DD3818                   2DD3818:"System\\Internet\\"
02DD36AD
02DD36B2
02DD36B7
02DD36BC
02DD36C1
02DD36C6
02DD36CB
02DD36CD
```

```
EAX      000000
EBX      02FC58
ECX      FFFFFF
EDX      02DB23
EBP      0019FA
ESP      0019F9
ESI      FFFFFF
EDI      02EFB4

EIP      02DD36

EFLAGS   002
ZF 0  PF 0
OF 0  SF 1
CF 0  TF 1

LastError   0
LastStatus  C
```

```
Address   Hex                                                  ASCII
02E35668  7C 46 E3 02 BC 25 AA 02 4C 26 AA 02 FC 50 E3 02  |Fã.¼%ª.L&ª.üPã.
02E35678  E0 EE E9 02 04 46 D1 02 14 47 D1 02 84 47 D1 02  àîé..FÑ..GÑ..GÑ.
02E35688  98 CA E3 02 6C 10 A5 02 88 70 FA 02 2C 4F E3 02  .Êã.l.¥..pú.,Oã.
```

```
Address   Hex                                                  ASCII
02E3467C  00 00 00 00 FF FF FF 7F 80 BA D7 02 00 00 00 00  ....ÿÿÿ..ºx.....
02E3468C  FF FF FF FF 00 C0 DA 44 00 00 FA 44 FF FF FF FF  ÿÿÿÿ.ÀÚD..úDÿÿÿÿ
02E3469C  06 00 00 00 33 33 73 3F 01 01 00 00 04 06 08 08  ....33s?........
```



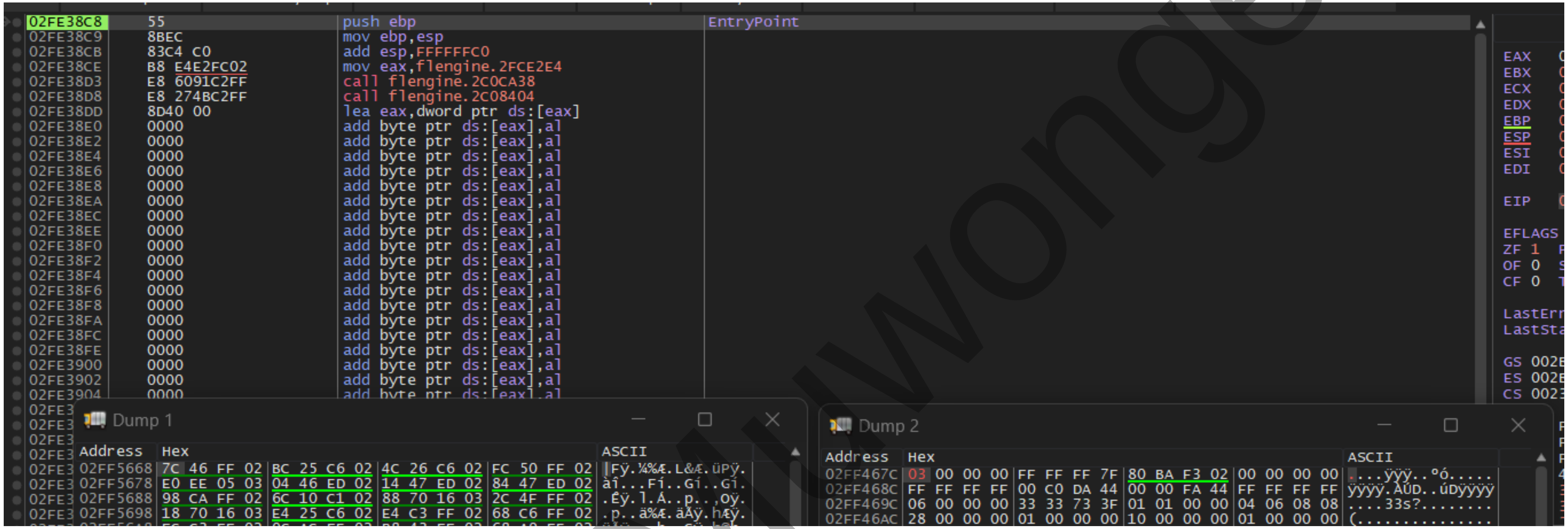
```
02D7C82B   833D 7C46E302 00        cmp dword ptr ds:[2E3467C],0
02D7C832   7E 3F                   jle flengine.2D7C873
02D7C834   833D 7C46E302 04        cmp dword ptr ds:[2E3467C],4
02D7C83B   7D 1B                   jge flengine.2D7C858
02D7C83D   B8 58D5F702             mov eax,flengine.2F7D558
02D7C842   BA 08CCD702             mov edx,flengine.2D7CC08           2D7CC08:"Upgrade registration"
02D7C847   E8 40C3CCFF             call flengine.2A48B8C
02D7C84C   C705 50D5F702 0100000   mov dword ptr ds:[2F7D550],1
02D7C856   EB 55                   jmp flengine.2D7C8AD
02D7C858   B8 58D5F702             mov eax,flengine.2F7D558
02D7C85D   BA 2CCCD702             mov edx,flengine.2D7CC2C           2D7CC2C:"Registration details"
02D7C862   E8 25C3CCFF             call flengine.2A48B8C
02D7C867   C705 50D5F702 0200000   mov dword ptr ds:[2F7D550],2
02D7C871   EB 3A                   jmp flengine.2D7C8AD
02D7C873   833D 3CD5F702 00        cmp dword ptr ds:[2F7D53C],0
02D7C87A   75 11                   jne flengine.2D7C88D
02D7C87C   B8 58D5F702             mov eax,flengine.2F7D558
02D7C881   BA 50CCD702             mov edx,flengine.2D7CC50           2D7CC50:"Buy / register"
02D7C886   E8 01C3CCFF             call flengine.2A48B8C
02D7C88B   EB 20                   jmp flengine.2D7C8AD
02D7C88D   33C0                    xor eax,eax
02D7C88F   A3 7C46E302             mov dword ptr ds:[2E3467C],eax
02D7C894
02D7C899
02D7C89E
02D7C8A3
02D7C8AD
02D7C8AF
02D7C8B0
02D7C8B1
```

```
EAX      02F7D53
EBX      0000000
ECX      0000000
EDX      0000000
EBP      0019F23
ESP      0019F20
ESI      02E3465
EDI      02F7D54

EIP      02D7C83

EFLAGS   0020
ZF 1  PF 1
OF 0  SF 0
CF 0  TF 1

LastError   00
LastStatus  C0
```

```
Address   Hex                                                  ASCII
02E35668  7C 46 E3 02 BC 25 AA 02 4C 26 AA 02 FC 50 E3 02  |Fã.¼%ª.L&ª.üPã.
02E35678  E0 EE E9 02 04 46 D1 02 14 47 D1 02 84 47 D1 02  àîé..FÑ..GÑ..GÑ.
02E35688  98 CA E3 02 6C 10 A5 02 88 70 FA 02 2C 4F E3 02  .Êã.l.¥..pú.,Oã.
02E35698  18 70 FA 02 E4 25 AA 02 E4 C3 E3 02 68 C6 E3 02  .pú.ä%ª.äÃã.hÆã.
```

```
Address   Hex                                                  ASCII
02E3467C  00 00 00 00 FF FF FF 7F 80 BA D7 02 00 00 00 00  ....ÿÿÿ..ºx.....
02E3468C  FF FF FF FF 00 C0 DA 44 00 00 FA 44 FF FF FF FF  ÿÿÿÿ.ÀÚD..úDÿÿÿÿ
02E3469C  06 00 00 00 33 33 73 3F 01 01 00 00 04 06 08 08  ....33s?........
02E346AC  28 00 00 00 01 00 00 00 10 00 00 00 01 00 00 00  (...............
```

Therefore setting the value at “Address #4” to “3” at the FLEngine.dll entry point will ensure FL Studio 11 Producer Edition gets loaded instead of the demo.



```
02FE38C8     55              push ebp                           EntryPoint
02FE38C9     8BEC            mov ebp,esp
02FE38CB     83C4 C0         add esp,FFFFFFC0
02FE38CE     B8 E4E2FC02     mov eax,flengine.2FCE2E4
02FE38D3     E8 6091C2FF     call flengine.2C0CA38
02FE38D8     E8 274BC2FF     call flengine.2C08404
02FE38DD     8D40 00         lea eax,dword ptr ds:[eax]
02FE38E0     0000            add byte ptr ds:[eax],al
02FE38E2     0000            add byte ptr ds:[eax],al
02FE38E4     0000            add byte ptr ds:[eax],al
02FE38E6     0000            add byte ptr ds:[eax],al
02FE38E8     0000            add byte ptr ds:[eax],al
02FE38EA     0000            add byte ptr ds:[eax],al
02FE38EC     0000            add byte ptr ds:[eax],al
02FE38EE     0000            add byte ptr ds:[eax],al
02FE38F0     0000            add byte ptr ds:[eax],al
02FE38F2     0000            add byte ptr ds:[eax],al
02FE38F4     0000            add byte ptr ds:[eax],al
02FE38F6     0000            add byte ptr ds:[eax],al
02FE38F8     0000            add byte ptr ds:[eax],al
02FE38FA     0000            add byte ptr ds:[eax],al
02FE38FC     0000            add byte ptr ds:[eax],al
02FE38FE     0000            add byte ptr ds:[eax],al
02FE3900     0000            add byte ptr ds:[eax],al
02FE3902     0000            add byte ptr ds:[eax],al
02FE3904     0000            add byte ptr ds:[eax],al
```

```
EAX
EBX
ECX
EDX
EBP
ESP
ESI
EDI

EIP

EFLAGS
ZF 1
OF 0
CF 0

LastErr
LastSta

GS 002E
ES 002E
CS 0023
```

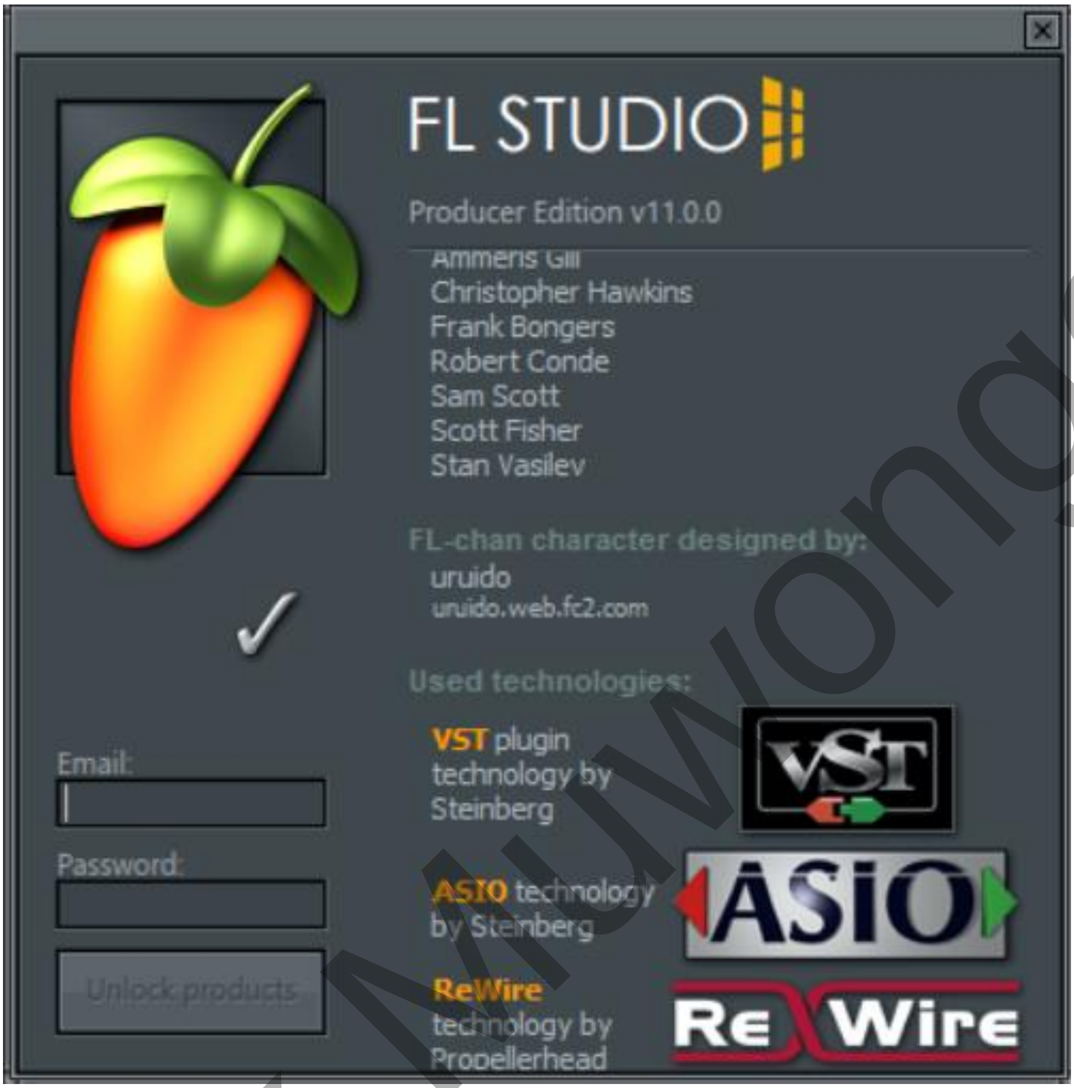
Dump 1

```
Address   Hex                                              ASCII
02FF5668  7C 46 FF 02 BC 25 C6 02 4C 26 C6 02 FC 50 FF 02  |Fÿ.¼%Æ.L&Æ.üPÿ.
02FF5678  E0 EE 05 03 04 46 ED 02 14 47 ED 02 84 47 ED 02  àî...Fí..Gí..Gí.
02FF5688  98 CA FF 02 6C 10 C1 02 88 70 16 03 2C 4F FF 02  .Êÿ.l.Á..p..,Oÿ.
02FF5698  18 70 16 03 E4 25 C6 02 E4 C3 FF 02 68 C6 FF 02  .p..ä%Æ.äÃÿ.hÆÿ.
```

Dump 2

```
Address   Hex                                              ASCII
02FF467C  03 00 00 00 FF FF FF 7F 80 BA F3 02 00 00 00 00  ....ÿÿÿ..ºó.....
02FF468C  FF FF FF FF 00 C0 DA 44 00 00 FA 44 FF FF FF FF  ÿÿÿÿ.ÀÚD..úDÿÿÿÿ
02FF469C  06 00 00 00 33 33 73 3F 01 01 00 00 04 06 08 08  ....33s?........
02FF46AC  28 00 00 00 01 00 00 00 10 00 00 00 01 00 00 00  (...............
```

FL Studio 11 Producer Edition



FL STUDIO 11

Producer Edition v11.0.0

Ammeris Gill
Christopher Hawkins
Frank Bongers
Robert Conde
Sam Scott
Scott Fisher
Stan Vasilev

FL-chan character designed by:
uruido
uruido.web.fc2.com

Used technologies:

VST plugin technology by Steinberg

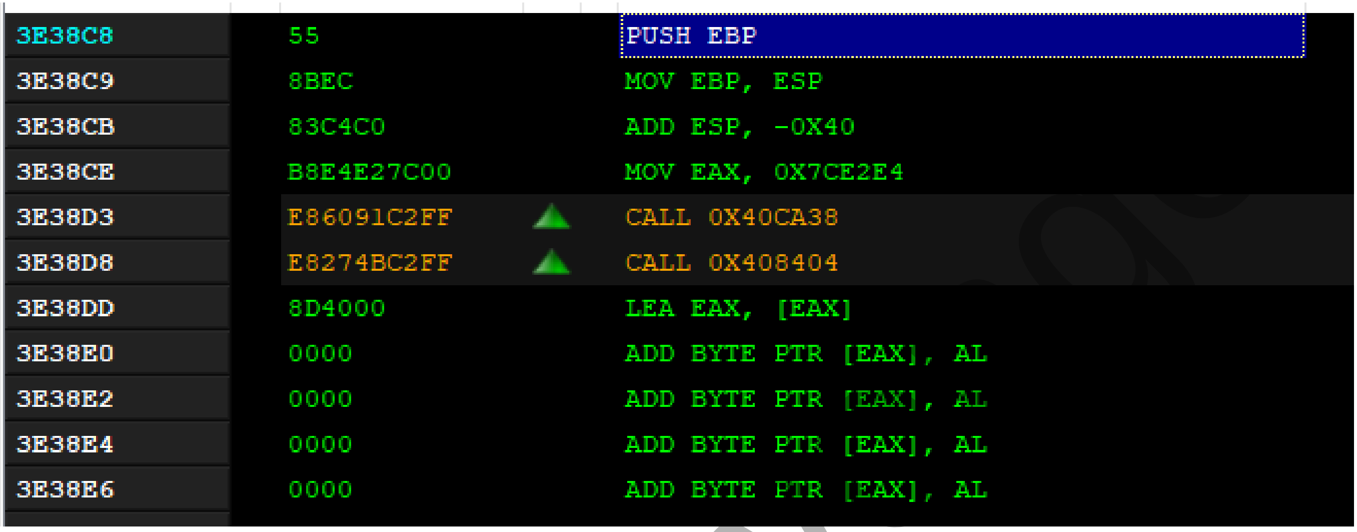
ASIO technology by Steinberg

ReWire technology by Propellerhead

Creating the Producer Edition patch

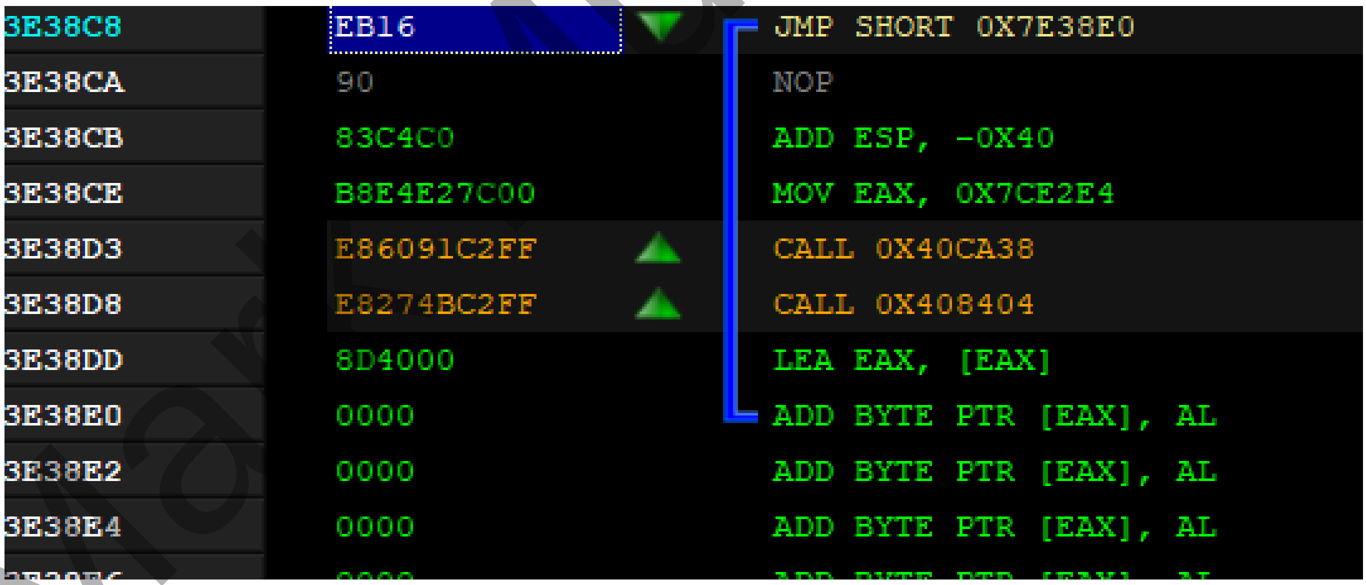
The patch is a replacement FLEngine.dll file that ensures the Producer Edition version gets loaded instead of the demo version. This is done by setting the default value at “Address #4” to three instead of zero.

Near the FLEngine.dll entry point, there are multiple of “padding bytes” that can be overwritten without affecting the execution of the program.



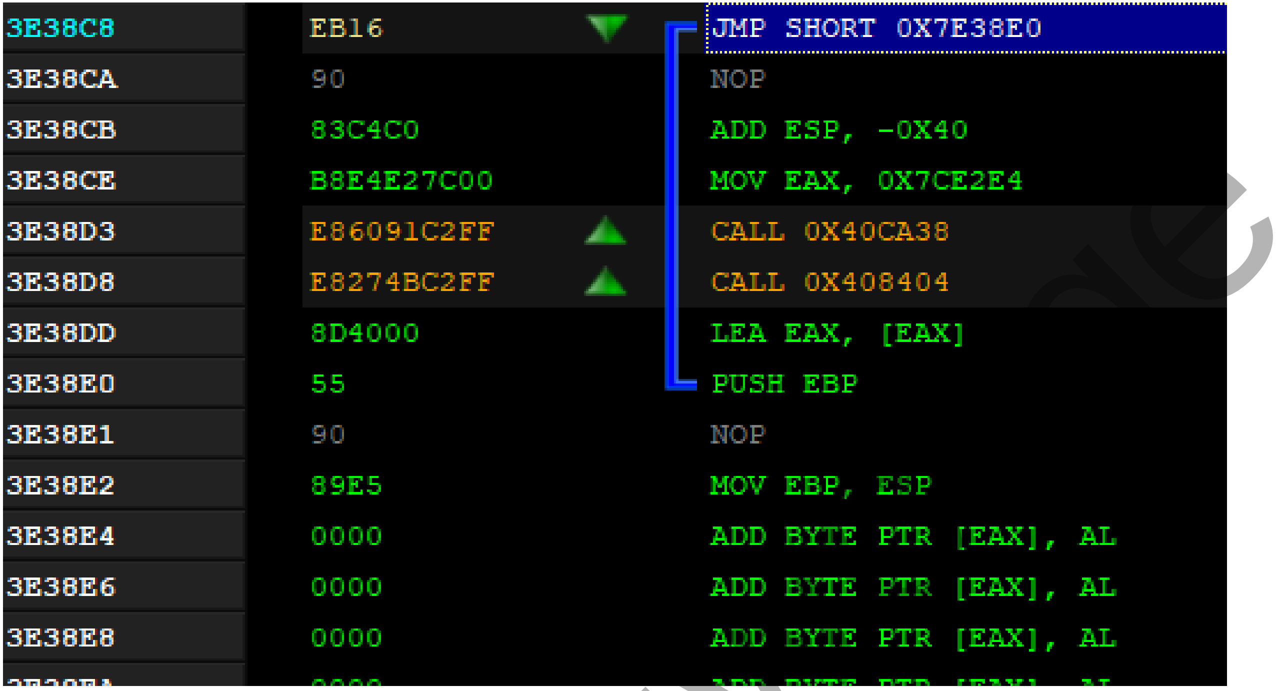
```
3E38C8    55            PUSH EBP
3E38C9    8BEC          MOV EBP, ESP
3E38CB    83C4C0        ADD ESP, -0X40
3E38CE    B8E4E27C00    MOV EAX, 0X7CE2E4
3E38D3    E86091C2FF    CALL 0X40CA38
3E38D8    E8274BC2FF    CALL 0X408404
3E38DD    8D4000        LEA EAX, [EAX]
3E38E0    0000          ADD BYTE PTR [EAX], AL
3E38E2    0000          ADD BYTE PTR [EAX], AL
3E38E4    0000          ADD BYTE PTR [EAX], AL
3E38E6    0000          ADD BYTE PTR [EAX], AL
```

Immediately transferring execution to the first byte of the “padding bytes” requires a two byte “short jump” instruction “0xEB, 0x16”. This will overwrite the “PUSH EBP” instruction however will only part overwrite the “MOV EBP, ESP” instruction which will in turn ruin the integrity of the subsequent instructions. Following the “short jump” instruction with a single byte “NOP” instruction solves this issue.



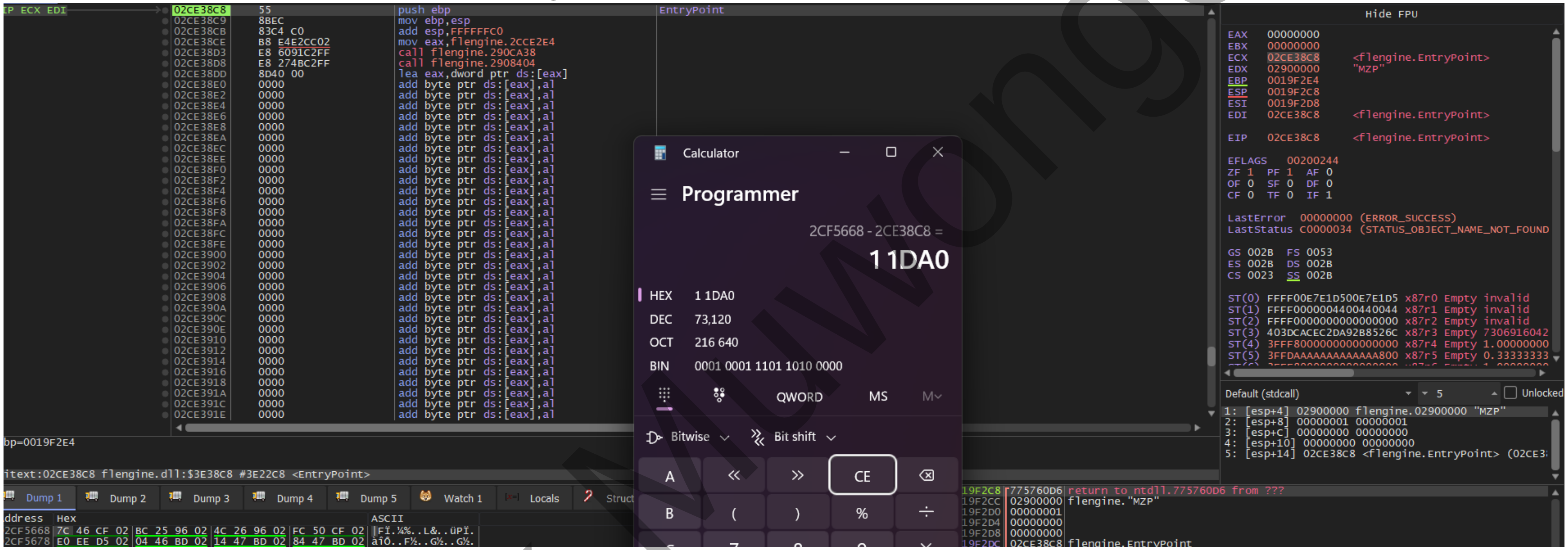
```
3E38C8    EB16          JMP SHORT 0X7E38E0
3E38CA    90            NOP
3E38CB    83C4C0        ADD ESP, -0X40
3E38CE    B8E4E27C00    MOV EAX, 0X7CE2E4
3E38D3    E86091C2FF    CALL 0X40CA38
3E38D8    E8274BC2FF    CALL 0X408404
3E38DD    8D4000        LEA EAX, [EAX]
3E38E0    0000          ADD BYTE PTR [EAX], AL
3E38E2    0000          ADD BYTE PTR [EAX], AL
3E38E4    0000          ADD BYTE PTR [EAX], AL
3E38E6    0000          ADD BYTE PTR [EAX], AL
```

Once the “short jump” has been made, the overwritten “PUSH EBP” and “MOV EBP, ESP” instructions are restored to ensure no state changes. As the addresses of the “padding bytes” fall on addresses that are a multiple of two and the “PUSH EBP” instruction is a single byte, a single “NOP” byte is placed after it.



```
3E38C8    EB16          JMP SHORT 0X7E38E0
3E38CA    90            NOP
3E38CB    83C4C0        ADD ESP, -0X40
3E38CE    B8E4E27C00    MOV EAX, 0X7CE2E4
3E38D3    E86091C2FF    CALL 0X40CA38
3E38D8    E8274BC2FF    CALL 0X408404
3E38DD    8D4000        LEA EAX, [EAX]
3E38E0    55            PUSH EBP
3E38E1    90            NOP
3E38E2    89E5          MOV EBP, ESP
3E38E4    0000          ADD BYTE PTR [EAX], AL
3E38E6    0000          ADD BYTE PTR [EAX], AL
3E38E8    0000          ADD BYTE PTR [EAX], AL
3E38EA    0000          ADD BYTE PTR [EAX], AL
```

The address of the FLEngine.dll entry point is conveniently present in the ECX register at the entry point. Calculating the difference between “Address #3” (holds the address to “Address #4” where the FL Studio 11 “version selector” is) and the FLEngine.dll entry point address and adding it to the value in the ECX register allows the “Address #4” to be accessed.



```
IP ECX EDI ──> 02CE38C8   55            push ebp                      EntryPoint
               02CE38C9   8BEC          mov ebp,esp
               02CE38CB   83C4 C0       add esp,FFFFFFC0
               02CE38CE   B8 E4E2CC02   mov eax,flengine.2CCE2E4
               02CE38D3   E8 6091C2FF   call flengine.290CA38
               02CE38D8   E8 274BC2FF   call flengine.2908404
               02CE38DD   8D40 00       lea eax,dword ptr ds:[eax]
               02CE38E0   0000          add byte ptr ds:[eax],al
               02CE38E2   0000          add byte ptr ds:[eax],al
               02CE38E4   0000          add byte ptr ds:[eax],al
               02CE38E6   0000          add byte ptr ds:[eax],al
               02CE38E8   0000          add byte ptr ds:[eax],al
               02CE38EA   0000          add byte ptr ds:[eax],al
               02CE38EC   0000          add byte ptr ds:[eax],al
               02CE38EE   0000          add byte ptr ds:[eax],al
               02CE38F0   0000          add byte ptr ds:[eax],al
               02CE38F2   0000          add byte ptr ds:[eax],al
               02CE38F4   0000          add byte ptr ds:[eax],al
               02CE38F6   0000          add byte ptr ds:[eax],al
               02CE38F8   0000          add byte ptr ds:[eax],al
               02CE38FA   0000          add byte ptr ds:[eax],al
               02CE38FC   0000          add byte ptr ds:[eax],al
               02CE38FE   0000          add byte ptr ds:[eax],al
               02CE3900   0000          add byte ptr ds:[eax],al
               02CE3902   0000          add byte ptr ds:[eax],al
               02CE3904   0000          add byte ptr ds:[eax],al
               02CE3906   0000          add byte ptr ds:[eax],al
               02CE3908   0000          add byte ptr ds:[eax],al
               02CE390A   0000          add byte ptr ds:[eax],al
               02CE390C   0000          add byte ptr ds:[eax],al
               02CE390E   0000          add byte ptr ds:[eax],al
               02CE3910   0000          add byte ptr ds:[eax],al
               02CE3912   0000          add byte ptr ds:[eax],al
               02CE3914   0000          add byte ptr ds:[eax],al
               02CE3916   0000          add byte ptr ds:[eax],al
               02CE3918   0000          add byte ptr ds:[eax],al
               02CE391A   0000          add byte ptr ds:[eax],al
               02CE391C   0000          add byte ptr ds:[eax],al
               02CE391E   0000          add byte ptr ds:[eax],al

bp=0019F2E4

itext:02CE38C8 flengine.dll:$3E38C8 #3E22C8 <EntryPoint>
```

```
ddress   Hex                                                  ASCII
2CF5668  7C 46 CF 02 BC 25 96 02 4C 26 96 02 FC 50 CF 02  |FÏ.¼%..L&..üPÏ.
2CF5678  E0 EE D5 02 04 46 BD 02 14 47 BD 02 84 47 BD 02  àîÕ..F½..G½..G½.
```

2CF5668 - 2CE38C8 =

1 1DA0

HEX 1 1DA0
DEC 73,120
OCT 216 640
BIN 0001 0001 1101 1010 0000

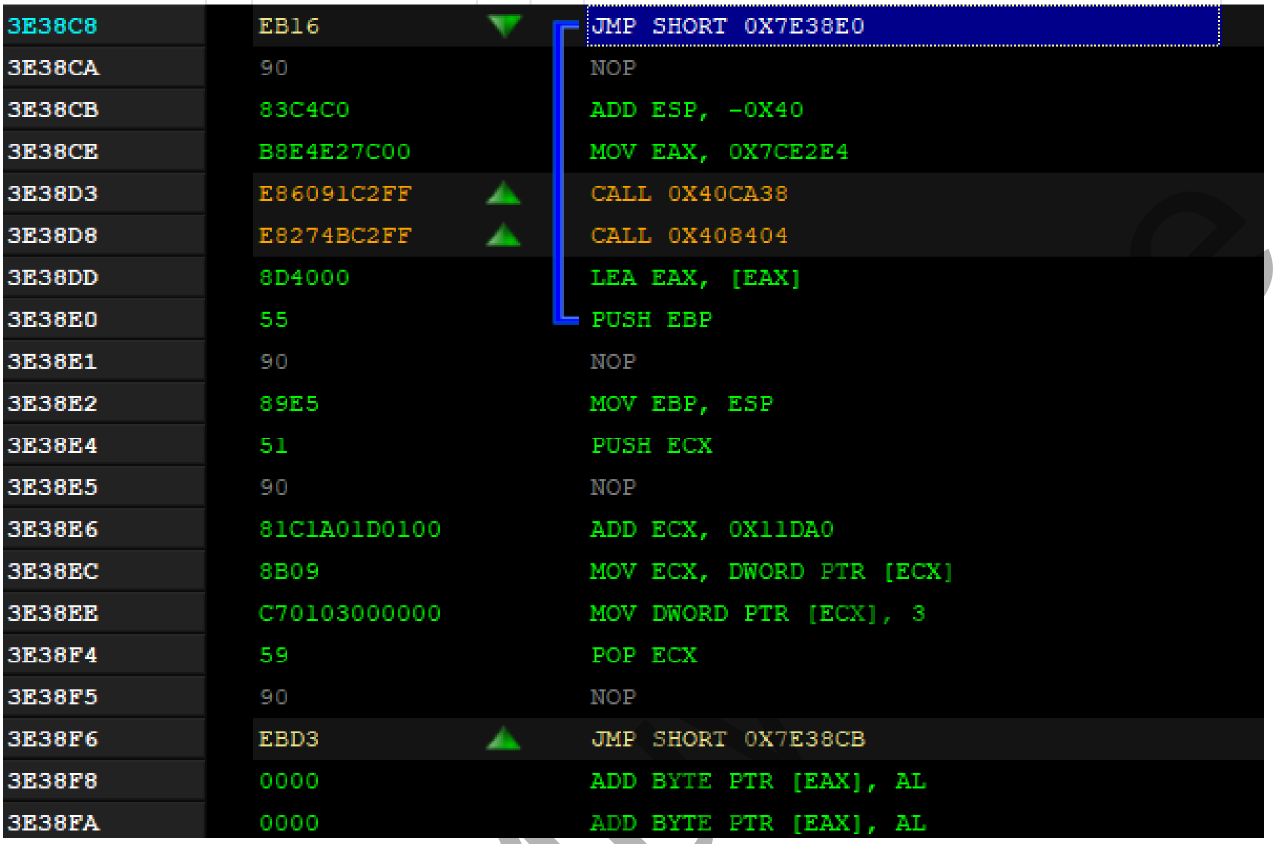
```
EAX   00000000
EBX   00000000
ECX   02CE38C8     <flengine.EntryPoint>
EDX   02900000     "MZP"
EBP   0019F2E4
ESP   0019F2C8
ESI   0019F2D8
EDI   02CE38C8     <flengine.EntryPoint>

EIP   02CE38C8     <flengine.EntryPoint>

EFLAGS   00200244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) FFFF00E7E1D500E7E1D5 x87r0 Empty invalid
ST(1) FFFF0000004400440044 x87r1 Empty invalid
ST(2) FFFF0000000000000000 x87r2 Empty invalid
ST(3) 403DCACEC2DA92B8526C x87r3 Empty 7306916042
ST(4) 3FFF8000000000000000 x87r4 Empty 1.00000000
ST(5) 3FFDAAAAAAAAAAAAA800 x87r5 Empty 0.33333333
```

Default (stdcall) 5 ☐ Unlocked

```
1: [esp+4] 02900000 flengine.02900000 "MZP"
2: [esp+8] 00000001 00000001
3: [esp+C] 00000000 00000000
4: [esp+10] 00000000 00000000
5: [esp+14] 02CE38C8 <flengine.EntryPoint> (02CE3
```

```
19F2C8 775760D6 return to ntdll.775760D6 from ???
19F2CC 02900000 flengine."MZP"
19F2D0 00000001
19F2D4 00000000
19F2D8 00000000
19F2DC 02CE38C8 flengine.EntryPoint
```

From there all that remains is to replace the “padding bytes” with instructions that set the value at “Address #4” to three and return to the third instruction from the FLEngine.dll entry point while maintaining byte alignment and the state of the registers.



```
3E38C8    EB16            JMP SHORT 0X7E38E0
3E38CA    90              NOP
3E38CB    83C4C0          ADD ESP, -0X40
3E38CE    B8E4E27C00      MOV EAX, 0X7CE2E4
3E38D3    E86091C2FF      CALL 0X40CA38
3E38D8    E8274BC2FF      CALL 0X408404
3E38DD    8D4000          LEA EAX, [EAX]
3E38E0    55              PUSH EBP
3E38E1    90              NOP
3E38E2    89E5            MOV EBP, ESP
3E38E4    51              PUSH ECX
3E38E5    90              NOP
3E38E6    81C1A01D0100    ADD ECX, 0X11DA0
3E38EC    8B09            MOV ECX, DWORD PTR [ECX]
3E38EE    C70103000000    MOV DWORD PTR [ECX], 3
3E38F4    59              POP ECX
3E38F5    90              NOP
3E38F6    EBD3            JMP SHORT 0X7E38CB
3E38F8    0000            ADD BYTE PTR [EAX], AL
3E38FA    0000            ADD BYTE PTR [EAX], AL
```