UPX 파일 디버깅

SCP 20학번 박준형

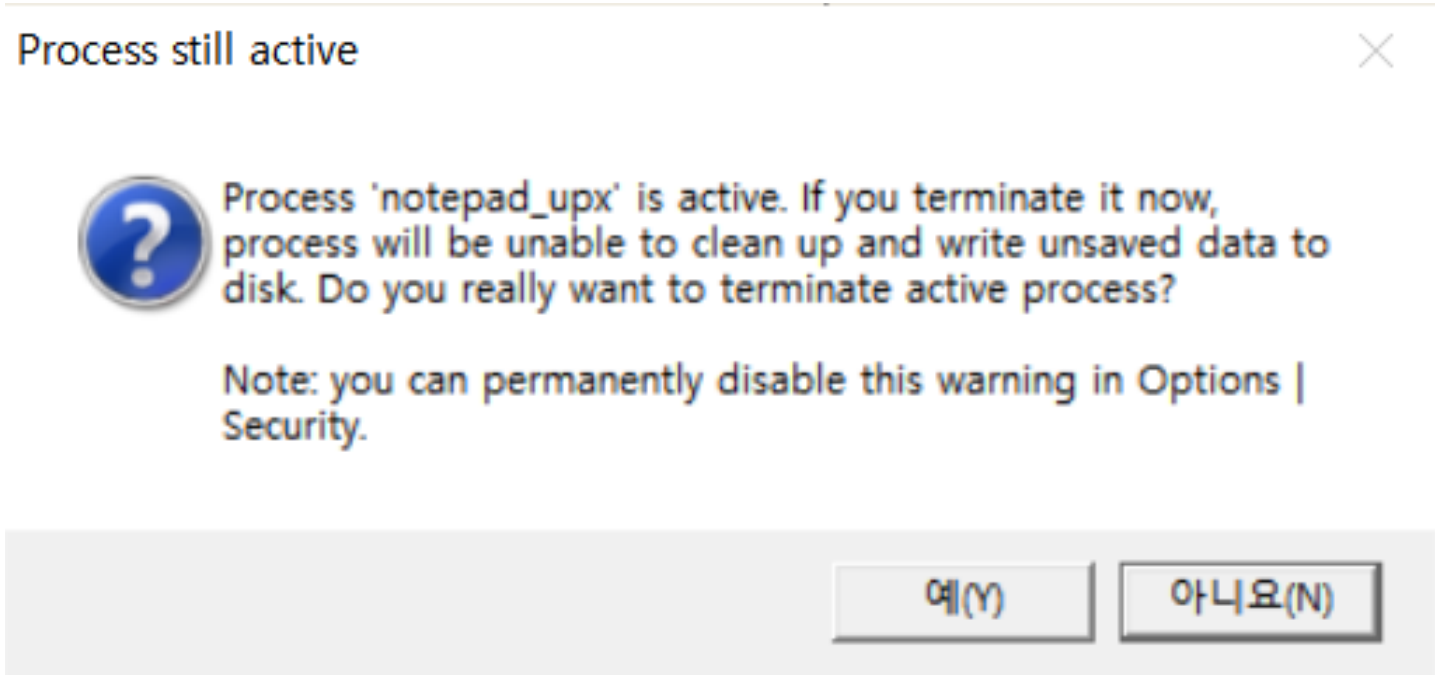
목차 table of contents

원본 파일과 UPX 파일 비교

Part 1 Notepad.exe의 EP 코드

```
0100739D  $ 6A 70          PUSH 70
0100739F  . 68 98180001    PUSH notepad.01001898
010073A4  . E8 BF010000    CALL notepad.01007568
010073A9  . 33DB           XOR EBX,EBX
010073AB  . 53             PUSH EBX                                 pModule => NULL
010073AC  . 8B3D CC100001  MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModu KERNEL32.GetModuleHandleA
010073B2  . FFD7           CALL EDI                                 GetModuleHandleA
010073B4  . 66:8138 4D5A   CMP WORD PTR DS:[EAX],5A4D  16진수)4D5A = MZ
010073B9  .v75 1F          JNZ SHORT notepad.010073DA
010073BB  . 8B48 3C        MOV ECX,DWORD PTR DS:[EAX+3C]
010073BE  . 03C8           ADD ECX,EAX
010073C0  . 8139 50450000  CMP DWORD PTR DS:[ECX],4550  16진수)5045 = PE
010073C6  .v75 12          JNZ SHORT notepad.010073DA
010073C8  . 0FB741 18      MOVZX EAX,WORD PTR DS:[ECX+18]
010073CC  . 3D 0B010000    CMP EAX,10B
010073D1  .v74 1F          JE SHORT notepad.010073F2
010073D3  . 3D 0B020000    CMP EAX,20B
010073D8  .v74 05          JE SHORT notepad.010073DF
010073DA  > 895D E4        MOV DWORD PTR SS:[EBP-1C],EBX
010073DD  .v EB 27         JMP SHORT notepad.01007406
010073DF  > 83B9 84000000  CMP DWORD PTR DS:[ECX+84],0E
010073E6  .^76 F2          JBE SHORT notepad.010073DA
010073E8  . 33C0           XOR EAX,EAX
010073EA  . 3999 F8000000  CMP DWORD PTR DS:[ECX+F8],EBX
010073F0  .v EB 0E         JMP SHORT notepad.01007400
010073F2  > 8379 74 0E     CMP DWORD PTR DS:[ECX+74],0E
010073F6  .^76 E2          JBE SHORT notepad.010073DA
010073F8  . 33C0           XOR EAX,EAX
010073FA  . 3999 E8000000  CMP DWORD PTR DS:[ECX+E8],EBX
```

Part 1 Notepad_upx.exe의 EP 코드



Part 1 Notepad_upx.exe의 EP 코드

```
01015330  $ 60            PUSHAD                          ← EP 코드
01015331  . BE 00100101   MOV ESI,notepad_.01011000
01015336  . 8DBE 0000FFFF LEA EDI,DWORD PTR DS:[ESI+FFFF0000]
0101533C  . 57            PUSH EDI
0101533D  . 83CD FF       OR EBP,FFFFFFFF
01015340  . EB 10         JMP SHORT notepad_.01015352
01015342    90            NOP
01015343    90            NOP
01015344    90            NOP
01015345    90            NOP
01015346    90            NOP
01015347    90            NOP
01015348  > 8A06          MOV AL,BYTE PTR DS:[ESI]
0101534A  . 46            INC ESI
0101534B  . 8807          MOV BYTE PTR DS:[EDI],AL
0101534D  . 47            INC EDI
0101534E  > 01DB          ADD EBX,EBX
01015350  . 75 07         JNZ SHORT notepad_.01015359
01015352  > 8B1E          MOV EBX,DWORD PTR DS:[ESI]
01015354  . 83EE FC       SUB ESI,-4
01015357  . 11DB          ADC EBX,EBX
01015359  > 72 ED         JB SHORT notepad_.01015348
0101535B  . B8 01000000   MOV EAX,1
01015360  > 01DB          ADD EBX,EBX
01015362  . 75 07         JNZ SHORT notepad_.0101536B
01015364  . 8B1E          MOV EBX,DWORD PTR DS:[ESI]
01015366  . 83EE FC       SUB ESI,-4
01015369  . 11DB          ADC EBX,EBX
0101536B  > 11C0          ADC EAX,EAX
```

Part 1 Notepad_upx.exe의 EP 코드

```
01015330  $ 60           PUSHAD                                  EAX ~ EDI 레지스터 값 저장
01015331  . BE 00100101   MOV ESI,notepad_.01011000              ESI와 EDI 레지스터를 각각 두 번째 섹션의
01015336  . 8DBE 0000FFFF LEA EDI,DWORD PTR DS:[ESI+FFFF0000]
0101533C  . 57           PUSH EDI
0101533D  . 83CD FF      OR EBP,FFFFFFFF
01015340  . EB 10        JMP SHORT notepad_.01015352
01015342    90           NOP
01015343    90           NOP
01015344    90           NOP
```

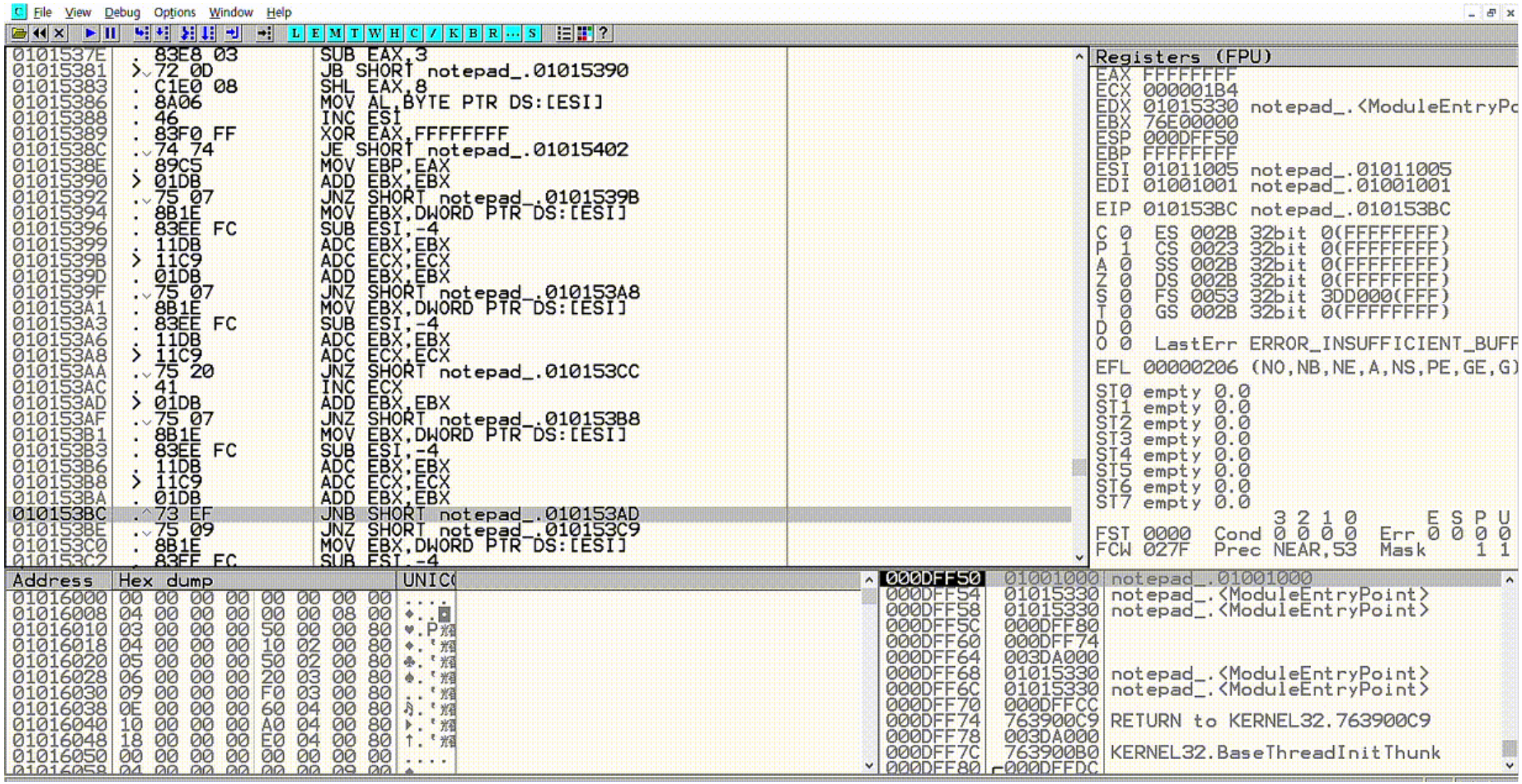
트레이싱 할 때 쓰는 Ollydbg 명령어

Part 2 트레이싱 할 때 쓰는 Ollydbg 명령어

명령어	단축키	설명
Animate Into	Ctrl+F7	Step Into 명령 반복(화면 표시 됨)
Animate Over	Ctrl+F8	Step Over 명령 반복(화면 표시 됨)
Trace Into	Ctrl+F11	Step Into 명령 반복(화면 표시 안 됨)
Trace Over	Ctrl+F12	Step Over 명령 반복(화면 표시 안 됨)

UPX 파일 트레이싱 실습

Part 3 루프#1


File View Debug Options Window Help
01015381 >v72 0D JB SHORT notepad_.01015390
01015383 . C1E0 08 SHL EAX,8
01015386 . 8A06 MOV AL,BYTE PTR DS:[ESI]
01015388 . 46 INC ESI
01015389 . 83F0 FF XOR EAX,FFFFFFFF
0101538C .v74 74 JE SHORT notepad_.01015402
0101538E . 89C5 MOV EBP,EAX
01015390 > 01DB ADD EBX,EBX
01015392 .v75 07 JNZ SHORT notepad_.0101539B
01015394 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
01015396 . 83EE FC SUB ESI,-4
01015399 . 11DB ADC EBX,EBX
0101539B > 11C9 ADC ECX,ECX
0101539D . 01DB ADD EBX,EBX
0101539F .v75 07 JNZ SHORT notepad_.010153A8
010153A1 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
010153A3 . 83EE FC SUB ESI,-4
010153A6 . 11DB ADC EBX,EBX
010153A8 > 11C9 ADC ECX,ECX
010153AA .v75 20 JNZ SHORT notepad_.010153CC
010153AC . 41 INC ECX
010153AD > 01DB ADD EBX,EBX
010153AF .v75 07 JNZ SHORT notepad_.010153B8
010153B1 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
010153B3 . 83EE FC SUB ESI,-4
010153B6 . 11DB ADC EBX,EBX
010153B8 > 11C9 ADC ECX,ECX
010153BA . 01DB ADD EBX,EBX
010153BC .^73 EF JNB SHORT notepad_.010153AD
010153BE .v75 09 JNZ SHORT notepad_.010153C9
010153C0 . 8B1E MOV EBX,DWORD PTR DS:[ESI]
Registers (FPU)
EAX FFFFFFFF
ECX 000001B4
EDX 01015330 notepad_.<ModuleEntryPo
EBX 76E00000
ESP 000DFF50
EBP FFFFFFFF
ESI 01011005 notepad_.01011005
EDI 01001001 notepad_.01001001
EIP 010153BC notepad_.010153BC
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 3DD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_INSUFFICIENT_BUFF
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U
FST 0000 Cond 0 0 0 0 Err 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1
Address Hex dump UNICO
01016000 00 00 00 00 00 00 00 00
01016008 04 00 00 00 00 00 08 00
01016010 03 00 00 00 50 00 00 80
01016018 04 00 00 00 10 02 00 80
01016020 05 00 00 00 50 02 00 80
01016028 06 00 00 00 20 03 00 80
01016030 09 00 00 00 F0 03 00 80
01016038 0E 00 00 00 60 04 00 80
01016040 10 00 00 00 A0 04 00 80
01016048 18 00 00 00 E0 04 00 80
01016050 00 00 00 00 00 00 00 00
000DFF50 01001000 notepad_.01001000
000DFF54 01015330 notepad_.<ModuleEntryPoint>
000DFF58 01015330 notepad_.<ModuleEntryPoint>
000DFF5C 000DFF80
000DFF60 000DFF74
000DFF64 003DA000
000DFF68 01015330 notepad_.<ModuleEntryPoint>
000DFF6C 01015330 notepad_.<ModuleEntryPoint>
000DFF70 000DFFCC
000DFF74 763900C9 RETURN to KERNEL32.763900C9
000DFF78 003DA000
000DFF7C 763900B0 KERNEL32.BaseThreadInitThunk
000DFF80 000DFFDC

Part 3 루프#1

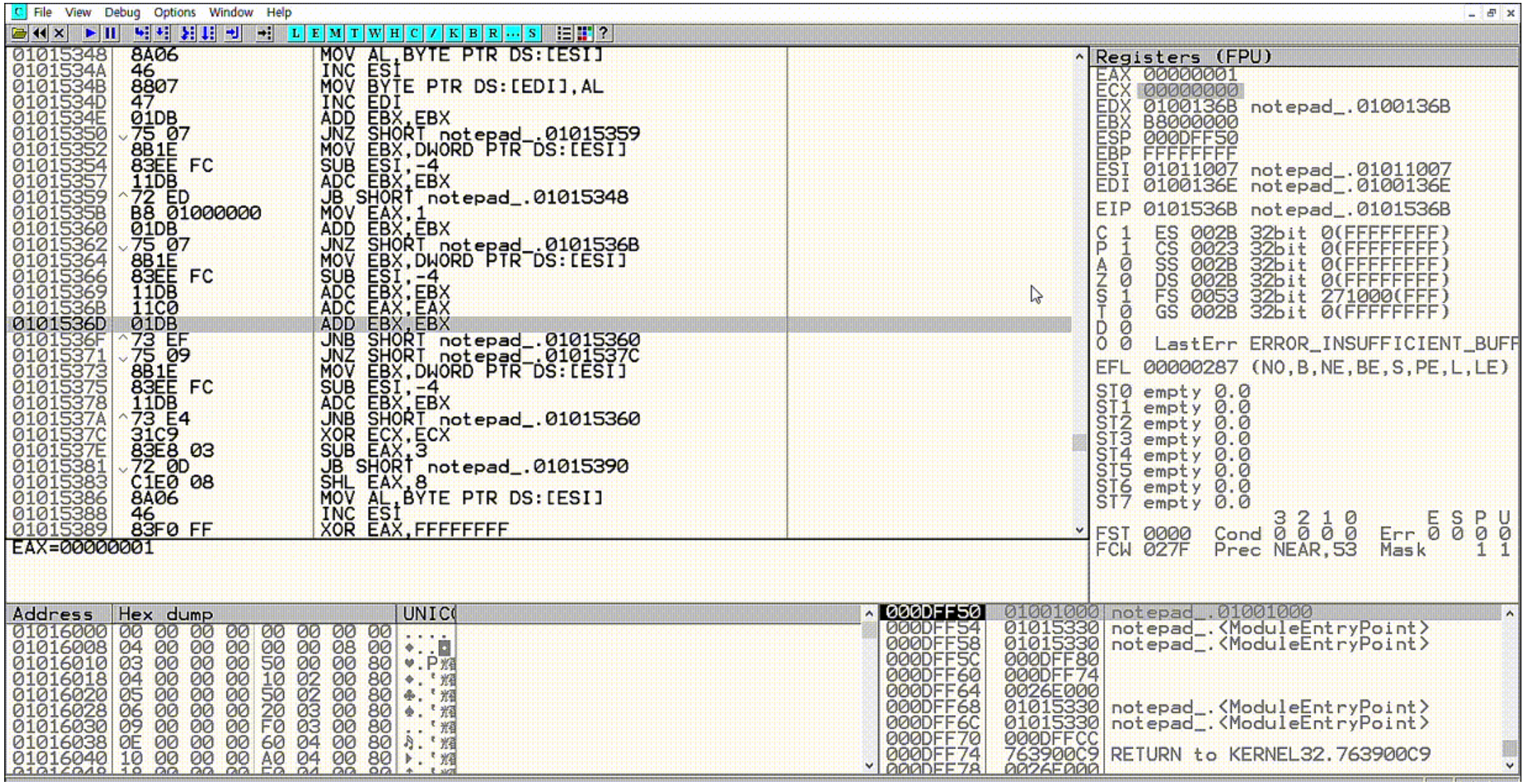
```
010153D8   83FD FC          CMP EBP,-4
010153DB   76 0F            JBE SHORT notepad_.010153EC
010153DD   8A02             MOV AL,BYTE PTR DS:[EDX]
010153DF   42               INC EDX
010153E0   8807             MOV BYTE PTR DS:[EDI],AL
010153E2   47               INC EDI
010153E3   49               DEC ECX
010153E4   ^75 F7           JNZ SHORT notepad_.010153DD
010153E6   ^E9 63FFFFFF     JMP notepad_.0101534E
010153EB   90               NOP
```

```
Registers (FPU)
EAX FFFFFFFF
ECX 0000036B 루프 회전 수
EDX 01001000 notepad_.01001000
EBX DB800000
ESP 000DFF50
EBP FFFFFFFF
ESI 01011005 notepad_.01011005
EDI 01001001 notepad_.01001001
```

```
010153D8   83FD FC          CMP EBP,-4
010153DB   76 0F            JBE SHORT not
010153DD   8A02             MOV AL,BYTE P
010153DF   42               INC EDX
010153E0   8807             MOV BYTE PTR
010153E2   47               INC EDI
010153E3   49               DEC ECX
010153E4   ^75 F7           JNZ SHORT not
010153E6   ^E9 63FFFFFF     JMP notepad_.
010153EB   90               NOP
```

(루프 탈출)

Part3 루프#2


File View Debug Options Window Help
01015348 8A06 MOV AL,BYTE PTR DS:[ESI]
0101534A 46 INC ESI
0101534B 8807 MOV BYTE PTR DS:[EDI],AL
0101534D 47 INC EDI
0101534E 01DB ADD EBX,EBX
01015350 75 07 JNZ SHORT notepad_.01015359
01015352 8B1E MOV EBX,DWORD PTR DS:[ESI]
01015354 83EE FC SUB ESI,-4
01015357 11DB ADC EBX,EBX
01015359 72 ED JB SHORT notepad_.01015348
0101535B B8 01000000 MOV EAX,1
01015360 01DB ADD EBX,EBX
01015362 75 07 JNZ SHORT notepad_.0101536B
01015364 8B1E MOV EBX,DWORD PTR DS:[ESI]
01015366 83EE FC SUB ESI,-4
01015369 11DB ADC EBX,EBX
0101536B 11C0 ADC EAX,EAX
0101536D 01DB ADD EBX,EBX
0101536F 73 EF JNB SHORT notepad_.01015360
01015371 75 09 JNZ SHORT notepad_.0101537C
01015373 8B1E MOV EBX,DWORD PTR DS:[ESI]
01015375 83EE FC SUB ESI,-4
01015378 11DB ADC EBX,EBX
0101537A 73 E4 JNB SHORT notepad_.01015360
0101537C 31C9 XOR ECX,ECX
0101537E 83E8 03 SUB EAX,3
01015381 72 0D JB SHORT notepad_.01015390
01015383 C1E0 08 SHL EAX,8
01015386 8A06 MOV AL,BYTE PTR DS:[ESI]
01015388 46 INC ESI
01015389 83F0 FF XOR EAX,FFFFFFFF
EAX=00000001
Registers (FPU)
EAX 00000001
ECX 00000000
EDX 0100136B notepad_.0100136B
EBX B8000000
ESP 000DFF50
EBP FFFFFFFF
ESI 01011007 notepad_.01011007
EDI 0100136E notepad_.0100136E
EIP 0101536B notepad_.0101536B
C 1 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 1 FS 0053 32bit 271000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_INSUFFICIENT_BUFF
EFL 00000287 (NO,B,NE,BE,S,PE,L,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U
FST 0000 Cond 0 0 0 0 Err 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1
Address Hex dump UNIC
01016000 00 00 00 00 00 00 00 00
01016008 04 00 00 00 00 00 08 00
01016010 03 00 00 00 50 00 00 80
01016018 04 00 00 00 10 02 00 80
01016020 05 00 00 00 50 02 00 80
01016028 06 00 00 00 20 03 00 80
01016030 09 00 00 00 F0 03 00 80
01016038 0E 00 00 00 60 04 00 80
01016040 10 00 00 00 A0 04 00 80
000DFF50 01001000 notepad_.01001000
000DFF54 01015330 notepad_.<ModuleEntryPoint>
000DFF58 01015330 notepad_.<ModuleEntryPoint>
000DFF5C 000DFF80
000DFF60 000DFF74
000DFF64 0026E000
000DFF68 01015330 notepad_.<ModuleEntryPoint>
000DFF6C 01015330 notepad_.<ModuleEntryPoint>
000DFF70 000DFFCC
000DFF74 763900C9 RETURN to KERNEL32.763900C9
000DFF78 0026E000

Part 3 루프#2

```
01015346   90              NOP
01015347   90              NOP
01015348   8A06            MOV AL,BYTE PTR DS:[ESI]
0101534A   46              INC ESI
0101534B   8807            MOV BYTE PTR DS:[EDI],AL
0101534D   47              INC EDI
0101534E   01DB            ADD EBX,EBX
01015350   75 07           JNZ SHORT notepad_.01015359
01015352   8B1E            MOV EBX,DWORD PTR DS:[ESI]
01015354   83EE FC         SUB ESI,-4
01015357   11DB            ADC EBX,EBX
01015359   72 ED           JB SHORT notepad_.01015348
0101535B   B8 01000000      MOV EAX,1
01015360   01DB            ADD EBX,EBX
01015362   75 07           JNZ SHORT notepad_.0101536B
01015364   8B1E            MOV EBX,DWORD PTR DS:[ESI]
01015366   83EE FC         SUB ESI,-4
01015369   11DB            ADC EBX,EBX
0101536B   11C0            ADC EAX,EAX
0101536D   01DB            ADD EBX,EBX
0101536F   73 EF           JNB SHORT notepad_.01015360
01015371   75 09           JNZ SHORT notepad_.0101537C
01015373   8B1E            MOV EBX,DWORD PTR DS:[ESI]
01015375   83EE FC         SUB ESI,-4
01015378   11DB            ADC EBX,EBX
0101537A   73 E4           JNB SHORT notepad_.01015360
0101537C   31C9            XOR ECX,ECX
```

Part 3 루프#2

(루프 탈출)

```
010153EE   83C2 04          ADD EDX,4
010153F1   8907             MOV DWORD PTR DS:[EDI],EAX
010153F3   83C7 04          ADD EDI,4
010153F6   83E9 04          SUB ECX,4
010153F9  ^77 F1            JA SHORT notepad_.010153EC
010153FB   01CF             ADD EDI,ECX
010153FD  ^E9 4CFFFFFF      JMP notepad_.0101534E
01015402   5E               POP ESI                          notepad_.01001000
01015403   89F7             MOV EDI,ESI
01015405   B9 32010000       MOV ECX,132
0101540A   8A07             MOV AL,BYTE PTR DS:[EDI]
0101540C   47               INC EDI
0101540D   2C E8            SUB AL,0E8
0101540F   3C 01            CMP AL,1
```

Part 3 루프#2

(루프 #2 실행 전)

Address	Hex dump	ASCII
01007000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01007090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

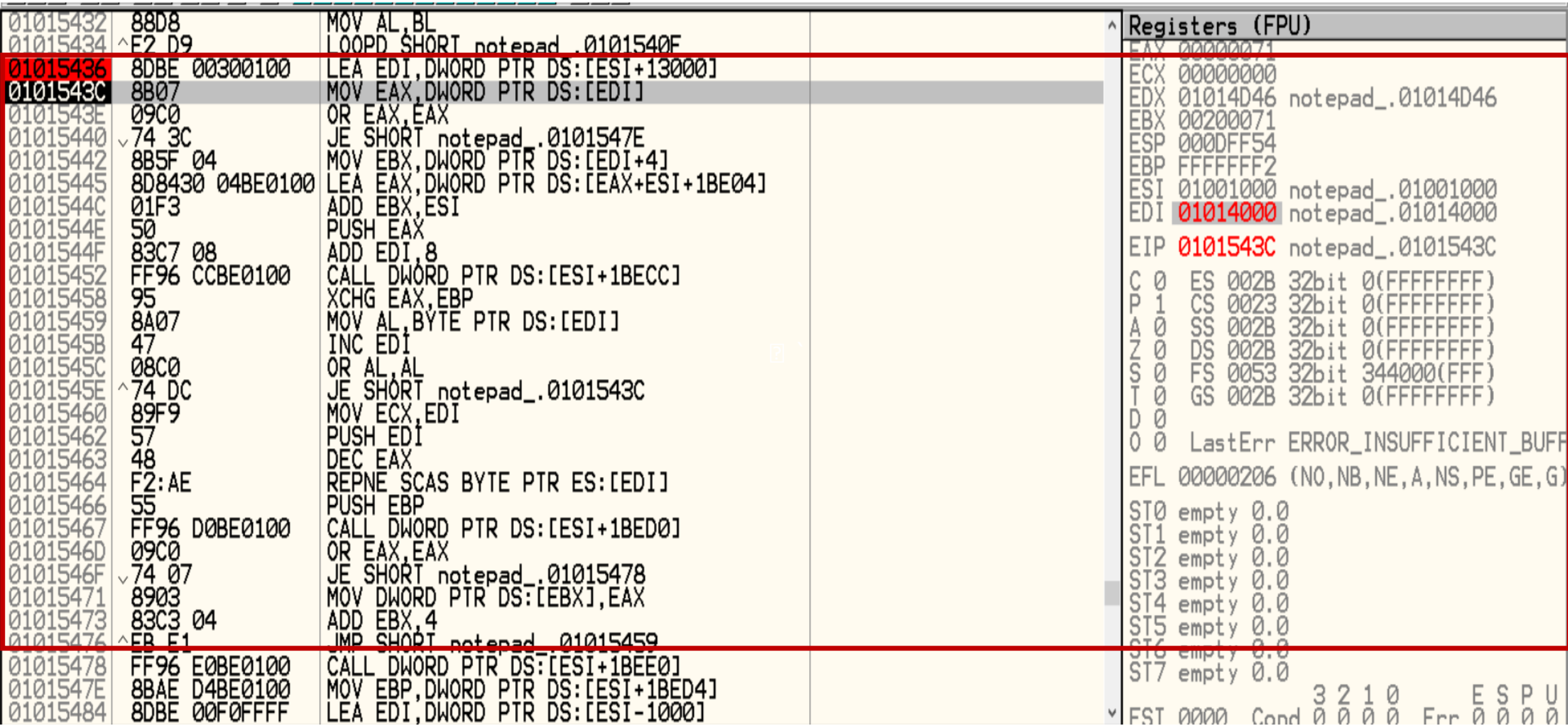
(루프 #2 실행 후)

Address	Hex dump	ASCII
01007000	18 00 01 8D 85 68 FD FF FF 50 FF D6 8D 85 28 FC	↑.┌뛇h? P ???(
01007010	FF FF 50 8D 85 68 FD FF FF 50 FF D6 39 5D 08 74	P뛇h? P 9]◘t
01007020	0A 57 8D 85 68 FD FF FF 50 FF D6 8D 85 68 FD FF	◙W뛇h? P ?뛇h?
01007030	FF 50 6A 01 68 C2 00 00 00 FF 35 38 98 00 01 FF	Pj┌h?.. 58?┌
01007040	15 40 12 00 01 8B 4D FC 5F 5E 5B E8 01 00 61 43	§@↕.┌딳?^[?.aC
01007050	C9 C2 04 00 CC CC CC CC CC 8B FF 55 8B EC 56 33	┘.儆儆? U뗭V3
01007060	F6 33 C9 46 33 D2 39 4D 0C 7E 35 8B 45 08 8A 04	??3?M.~5딜◘?
01007070	01 84 C0 79 02 33 F6 85 D2 75 10 3C 80 72 13 D0	┌쫿y┐3??┼<r‼?
01007080	E0 42 84 C0 78 F9 4A 74 17 EB 07 24 C0 3C 80 75	?쫿x?t┤?$?u
01007090	0F 4A 41 3B 4D 0C 7C D3 85 D2 77 04 85 F6 74 04	☼JA;M.\??┘깈t┘
010070A0	33 C0 EB 03 33 C0 40 5E 5D C2 08 00 CC CC CC CC	3잼└3?^]?.儆儆
010070B0	CC 8B FF 55 8B EC 51 83 4D FC FF 8D 45 FC 50 FF	? U뗭Q긎?뛇?

Part 3 루프#3

```
01015403   89F7              MOV EDI,ESI
01015405   B9 32010000        MOV ECX,132
0101540A   8A07              MOV AL,BYTE PTR DS:[EDI]
0101540C   47                INC EDI
0101540D   2C E8             SUB AL,0E8
0101540F   3C 01             CMP AL,1
01015411 ^ 77 F7             JA SHORT notepad_.0101540A
01015413   803F 01           CMP BYTE PTR DS:[EDI],1
01015416 ^ 75 F2             JNZ SHORT notepad_.0101540A
01015418   8B07              MOV EAX,DWORD PTR DS:[EDI]
0101541A   8A5F 04           MOV BL,BYTE PTR DS:[EDI+4]
0101541D   66:C1E8 08        SHR AX,8
01015421   C1C0 10           ROL EAX,10
01015424   86C4              XCHG AH,AL
01015426   29F8              SUB EAX,EDI
01015428   80EB E8           SUB BL,0E8
0101542B   01F0              ADD EAX,ESI
0101542D   8907              MOV DWORD PTR DS:[EDI],EAX
0101542F   83C7 05           ADD EDI,5
01015432   88D8              MOV AL,BL
01015434 ^ E2 D9             LOOPD SHORT notepad_.0101540F
01015436   8DBE 00300100     LEA EDI,DWORD PTR DS:[ESI+13000]
0101543C   8B07              MOV EAX,DWORD PTR DS:[EDI]
0101543E   09C0              OR EAX,EAX
01015440 v 74 3C             JE SHORT notepad_.0101547E
01015442   8B5F 04           MOV EBX,DWORD PTR DS:[EDI+4]
```

Part 3 루프#4

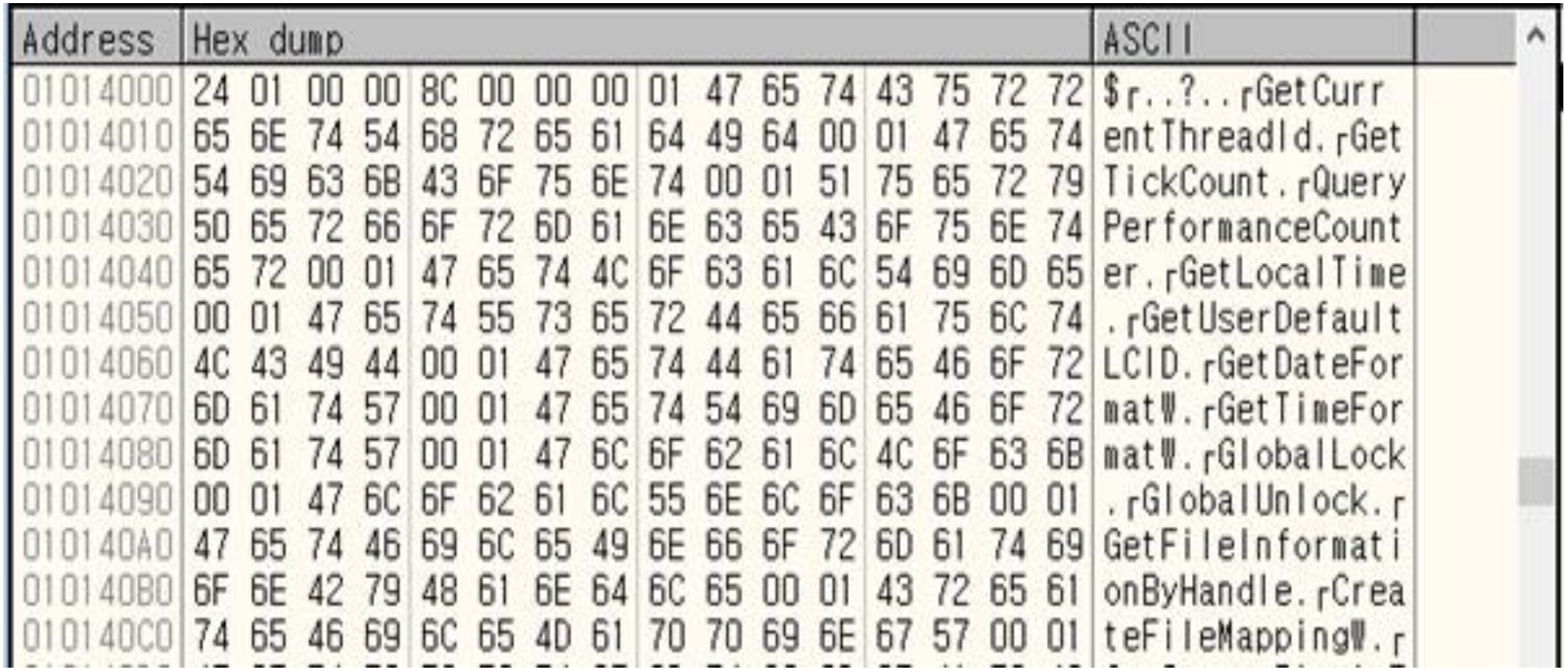

01015432 88D8 MOV AL,BL
01015434 ^E2 D9 LOOPD SHORT notepad_.0101540F
01015436 8DBE 00300100 LEA EDI,DWORD PTR DS:[ESI+13000]
0101543C 8B07 MOV EAX,DWORD PTR DS:[EDI]
0101543E 09C0 OR EAX,EAX
01015440 74 3C JE SHORT notepad_.0101547E
01015442 8B5F 04 MOV EBX,DWORD PTR DS:[EDI+4]
01015445 8D8430 04BE0100 LEA EAX,DWORD PTR DS:[EAX+ESI+1BE04]
0101544C 01F3 ADD EBX,ESI
0101544E 50 PUSH EAX
0101544F 83C7 08 ADD EDI,8
01015452 FF96 CCBE0100 CALL DWORD PTR DS:[ESI+1BECC]
01015458 95 XCHG EAX,EBP
01015459 8A07 MOV AL,BYTE PTR DS:[EDI]
0101545B 47 INC EDI
0101545C 08C0 OR AL,AL
0101545E ^74 DC JE SHORT notepad_.0101543C
01015460 89F9 MOV ECX,EDI
01015462 57 PUSH EDI
01015463 48 DEC EAX
01015464 F2:AE REPNE SCAS BYTE PTR ES:[EDI]
01015466 55 PUSH EBP
01015467 FF96 D0BE0100 CALL DWORD PTR DS:[ESI+1BED0]
0101546D 09C0 OR EAX,EAX
0101546F 74 07 JE SHORT notepad_.01015478
01015471 8903 MOV DWORD PTR DS:[EBX],EAX
01015473 83C3 04 ADD EBX,4
01015476 ^EB E1 JMP SHORT notepad_.01015459
01015478 FF96 E0BE0100 CALL DWORD PTR DS:[ESI+1BEE0]
0101547E 8BAE D4BE0100 MOV EBP,DWORD PTR DS:[ESI+1BED4]
01015484 8DBE 00F0FFFF LEA EDI,DWORD PTR DS:[ESI-1000]
Registers (FPU)
EAX 00000071
ECX 00000000
EDX 01014D46 notepad_.01014D46
EBX 00200071
ESP 000DFF54
EBP FFFFFFF2
ESI 01001000 notepad_.01001000
EDI 01014000 notepad_.01014000
EIP 0101543C notepad_.0101543C
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 344000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_INSUFFICIENT_BUFF
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U
FST 0000 Cond 0 0 0 0 Err 0 0 0 0

Part 3 루프#4

```
01015432   88D8              MOV AL,BL
01015434  ^E2 D9             LOOPD SHORT notepad_.0101540F
01015436   8DBE 00300100     LEA EDI,DWORD PTR DS:[ESI+13000]
0101543C   8B07              MOV EAX,DWORD PTR DS:[EDI]
0101543E   09C0              OR EAX,EAX
01015440  v74 3C             JE SHORT notepad_.0101547E
01015442   8B5F 04           MOV EBX,DWORD PTR DS:[EDI+4]
01015445   8D8430 04BE0100   LEA EAX,DWORD PTR DS:[EAX+ESI+1BE04]
0101544C   01F3              ADD EBX,ESI
0101544E   50                PUSH EAX
0101544F   83C7 08           ADD EDI,8
01015452   FF96 CCBE0100     CALL DWORD PTR DS:[ESI+1BECC]
01015458   95                XCHG EAX,EBP
01015459   8A07              MOV AL,BYTE PTR DS:[EDI]
0101545B   47                INC EDI
0101545C   08C0              OR AL,AL
0101545E  ^74 DC             JE SHORT notepad_.0101543C
01015460   89F9              MOV ECX,EDI
01015462   57                PUSH EDI
01015463   48                DEC EAX
01015464   F2:AE             REPNE SCAS BYTE PTR ES:[EDI]
01015466   55                PUSH EBP
01015467   FF96 D0BE0100     CALL DWORD PTR DS:[ESI+1BED0]
0101546D   09C0              OR EAX,EAX
0101546F  v74 07             JE SHORT notepad_.01015478
01015471   8903              MOV DWORD PTR DS:[EBX],EAX
01015473   83C3 04           ADD EBX,4
01015476  ^EB E1             JMP SHORT notepad_.01015459
01015478   FF96 E0BE0100     CALL DWORD PTR DS:[ESI+1BEE0]
0101547E   8BAE D4BE0100     MOV EBP,DWORD PTR DS:[ESI+1BED4]
01015484   8DBE 00F0FFFF     LEA EDI,DWORD PTR DS:[ESI-1000]
```

```
Registers (FPU)
EAX 00000071
ECX 00000000
EDX 01014D46 notepad_.01014D46
EBX 00200071
ESP 000DFF54
EBP FFFFFFF2
ESI 01001000 notepad_.01001000
EDI 01014000 notepad_.01014000

EIP 0101543C notepad_.0101543C

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 227000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_INSUFFICIENT_BUFF

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U
FST 0000  Cond 0 0 0 0  Err 0 0 0 0
```

Part 3 루프#4



Address	Hex dump	ASCII
01014000	24 01 00 00 8C 00 00 00 01 47 65 74 43 75 72 72	$┌..?..┌GetCurr
01014010	65 6E 74 54 68 72 65 61 64 49 64 00 01 47 65 74	entThreadId.┌Get
01014020	54 69 63 6B 43 6F 75 6E 74 00 01 51 75 65 72 79	TickCount.┌Query
01014030	50 65 72 66 6F 72 6D 61 6E 63 65 43 6F 75 6E 74	PerformanceCount
01014040	65 72 00 01 47 65 74 4C 6F 63 61 6C 54 69 6D 65	er.┌GetLocalTime
01014050	00 01 47 65 74 55 73 65 72 44 65 66 61 75 6C 74	.┌GetUserDefault
01014060	4C 43 49 44 00 01 47 65 74 44 61 74 65 46 6F 72	LCID.┌GetDateFor
01014070	6D 61 74 57 00 01 47 65 74 54 69 6D 65 46 6F 72	matW.┌GetTimeFor
01014080	6D 61 74 57 00 01 47 6C 6F 62 61 6C 4C 6F 63 6B	matW.┌GlobalLock
01014090	00 01 47 6C 6F 62 61 6C 55 6E 6C 6F 63 6B 00 01	.┌GlobalUnlock.┌
010140A0	47 65 74 46 69 6C 65 49 6E 66 6F 72 6D 61 74 69	GetFileInformati
010140B0	6F 6E 42 79 48 61 6E 64 6C 65 00 01 43 72 65 61	onByHandle.┌Crea
010140C0	74 65 46 69 6C 65 4D 61 70 70 69 6E 67 57 00 01	teFileMappingW.┌

Part 3 루프#4

```
010154AD   61              POPAD
010154AE   8D4424 80       LEA EAX,DWORD PTR SS:[ESP-80]
010154B2   6A 00           PUSH 0
010154B4   39C4            CMP ESP,EAX
010154B6  ^75 FA           JNZ SHORT notepad_.010154B2
010154B8   83EC 80         SUB ESP,-80
010154BB  -E9 DD1EFFFF     JMP notepad_.0100739D
```

OllyDbg - notepad.exe - [CPU - main thread, module notepad]

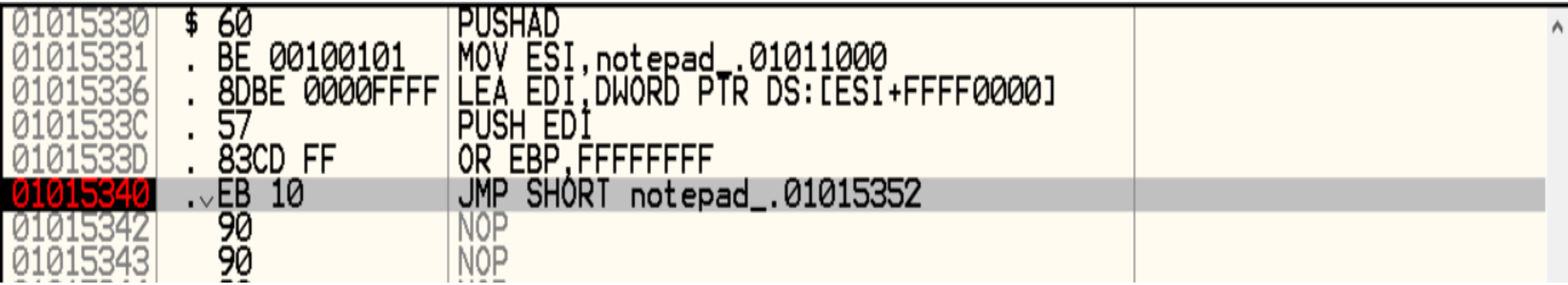
File View Debug Options Window Help

```
0100739D   $ 6A 70         PUSH 70
010073A0   . 68 98180001   PUSH notepad.01001898
010073A4   . E8 BF010000   CALL notepad.01007568
010073A9   . 33DB          XOR EBX,EBX
010073AB   . 53            PUSH EBX
010073AC   . 8B3D CC100001 MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModu  pModule => NULL
010073B2   . FFD7          CALL EDI                                   KERNEL32.GetModuleHand
010073B4   . 66:8138 4D5A  CMP WORD PTR DS:[EAX],5A4D                 GetModuleHandleA
010073B9   .v75 1F         JNZ SHORT notepad.010073DA
010073BB   . 8B48 3C       MOV ECX,DWORD PTR DS:[EAX+3C]
010073BE   . 03C8          ADD ECX,EAX
010073C0   . 8139 50450000 CMP DWORD PTR DS:[ECX],4550
```

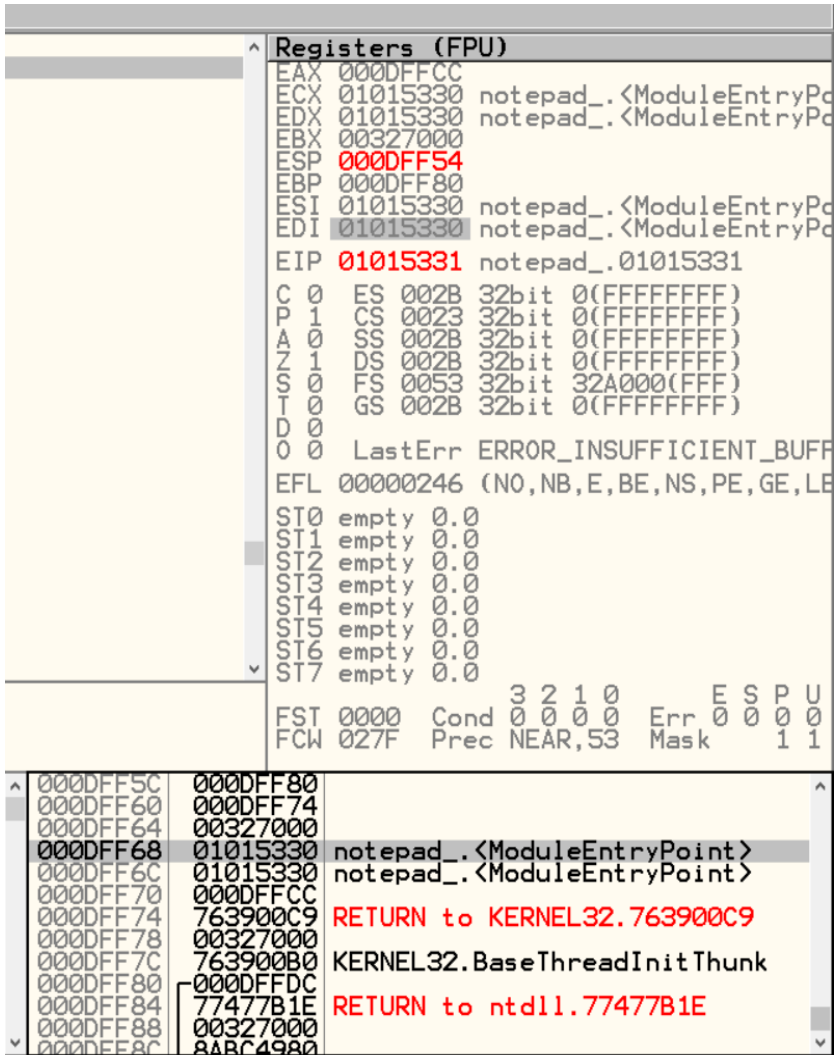
UPX의 OEP를 빨리 찾는 방법

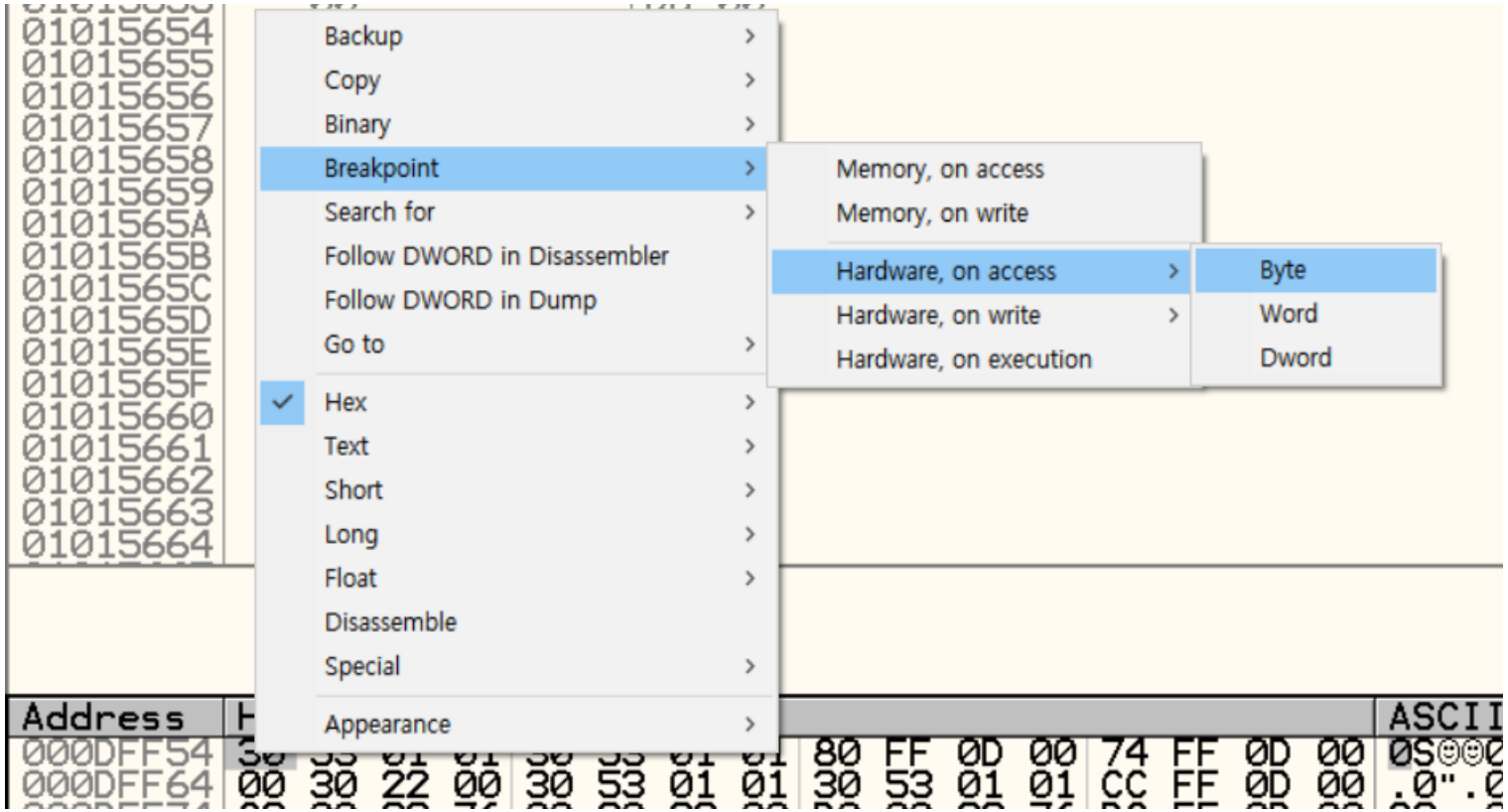
1. POPAD 명령어 이후의 JMP 명령어에 BP 설치

OEP코드로 가는 JMP 명령어가 POPAD 명령어 바로 이후에 나타나기에, 이 JMP명령어에 BP를 설치하고 실행하면 바로 OEP로 갈 수 있다.



2. 스택에 하드웨어 브레이크포인트 설치





Q&A