BASIC RCE Level 5

CodeEngn
ReverseEngineering Conference

2013 07/13
Malcook90@naver.com

Challenges : Basic 05

Author : Acid Bytes [CFF]

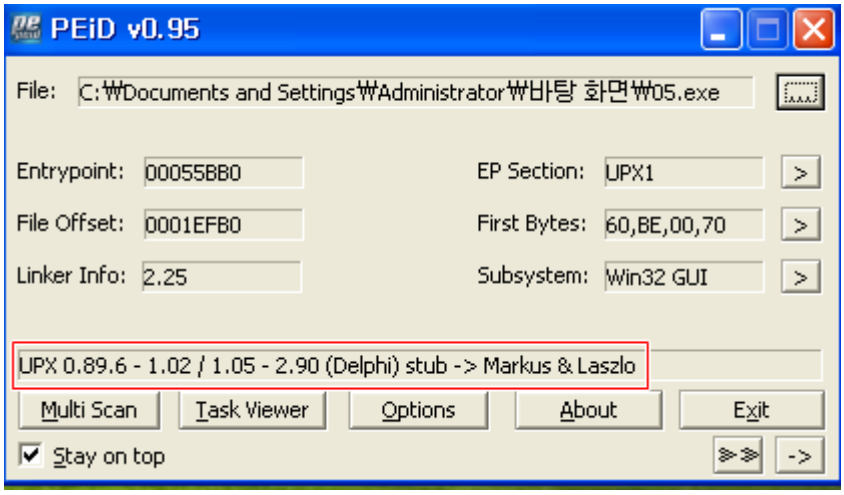
Korea :
이 프로그램의 등록키는 무엇인가

English :
The registration key of this program is?

문제는 파악했으니.. 한번 프로그램을 실행시켜 보겠습니다.

간단하게 표현해서 ID/PW 찾아서 성공메시지 을 띄어줘야 하는(?)

프로그램 인걸 알 수 있습니다.



– 패킹 결과 (여기서는 패킹되어 있다는 것을 알고 있다는 전제하에 진행)

위와 같이 UPX 로 패킹되어 있다는 것을 알 수 있습니다.

UPX 많이 알려진 패킹방법 중 하나로 간단히 Tool 로도 풀 수 있지만

여기서는 OllyDBG 로 코드을 따라가서 결과값을 알아 보겠습니다.

```
00455BB0  $  60              PUSHAD
00455BB1  .  BE 00704300     MOV ESI,05.00437000
00455BB6  .  8DBE 00A0FCFF   LEA EDI,DWORD PTR DS:[ESI+FFFCA000]
00455BBC  .  C787 D0024040   MOV DWORD PTR DS:[EDI+424D0],689C0471
00455BC6  .  57              PUSH EDI
00455BC7  .  83CD FF         OR EBP,FFFFFFFF
00455BCA  .v EB 0E           JMP SHORT 05.00455BDA
00455BCC     90              NOP
00455BCD     90              NOP
00455BCE     90              NOP
00455BCF     90              NOP
00455BD0  >  8A06            MOV AL,BYTE PTR DS:[ESI]
00455BD2  .  46              INC ESI
00455BD3  .  8807            MOV BYTE PTR DS:[EDI],AL
00455BD5  .  47              INC EDI
00455BD6  >  01DB            ADD EBX,EBX
00455BD8  .v 75 07           JNZ SHORT 05.00455BE1
00455BDA  >  8B1E            MOV EBX,DWORD PTR DS:[ESI]
00455BDC  .  83EE FC         SUB ESI,-4
00455BDF  .  11DB            ADC EBX,EBX
00455BE1  >^ 72 ED           JB SHORT 05.00455BD0
00455BE3  .  B8 01000000     MOV EAX,1
00455BE8  >  01DB            ADD EBX,EBX
00455BEA  .v 75 07           JNZ SHORT 05.00455BF3
```

실행시 첫 주소값 이며 여기에서 String 값을 볼려고 해도 아무것도 잡히질 않습니다.

```
00455CE4  .  08C0          OR AL,AL
00455CE6  .^ 74 DC         JE SHORT 05.00455CC4
00455CE8  .  89F9          MOV ECX,EDI
00455CEA  .  57            PUSH EDI
00455CEB  .  48            DEC EAX
00455CEC  .  F2:AE         REPNE SCAS BYTE PTR ES:[EDI]
00455CEE  .  55            PUSH EBP
00455CEF  .  FF96 0061050( CALL DWORD PTR DS:[ESI+56100]
00455CF5  .  09C0          OR EAX,EAX
00455CF7  .v 74 07         JE SHORT 05.00455D00
00455CF9  .  8903          MOV DWORD PTR DS:[EBX],EAX
00455CFB  .  83C3 04       ADD EBX,4
00455CFE  .^ EB E1         JMP SHORT 05.00455CE1
00455D00  >  FF96 0461050( CALL DWORD PTR DS:[ESI+56104]
00455D06  >  61            POPAD
00455D07  .^ E9 64B5FEFF   JMP 05.00441270
00455D0C     245D4500      DD 05.00455D24
00455D10     345D4500      DD 05.00455D34
00455D14     D0344400      DD 05.004434D0
00455D18     00            DB 00
00455D19     00            DB 00
00455D1A     00            DB 00
00455D1B     00            DB 00
00455D1C     00            DB 00
```

소스을 보면서 조금 내려가다 다음과 같은 명령어가 있습니다.

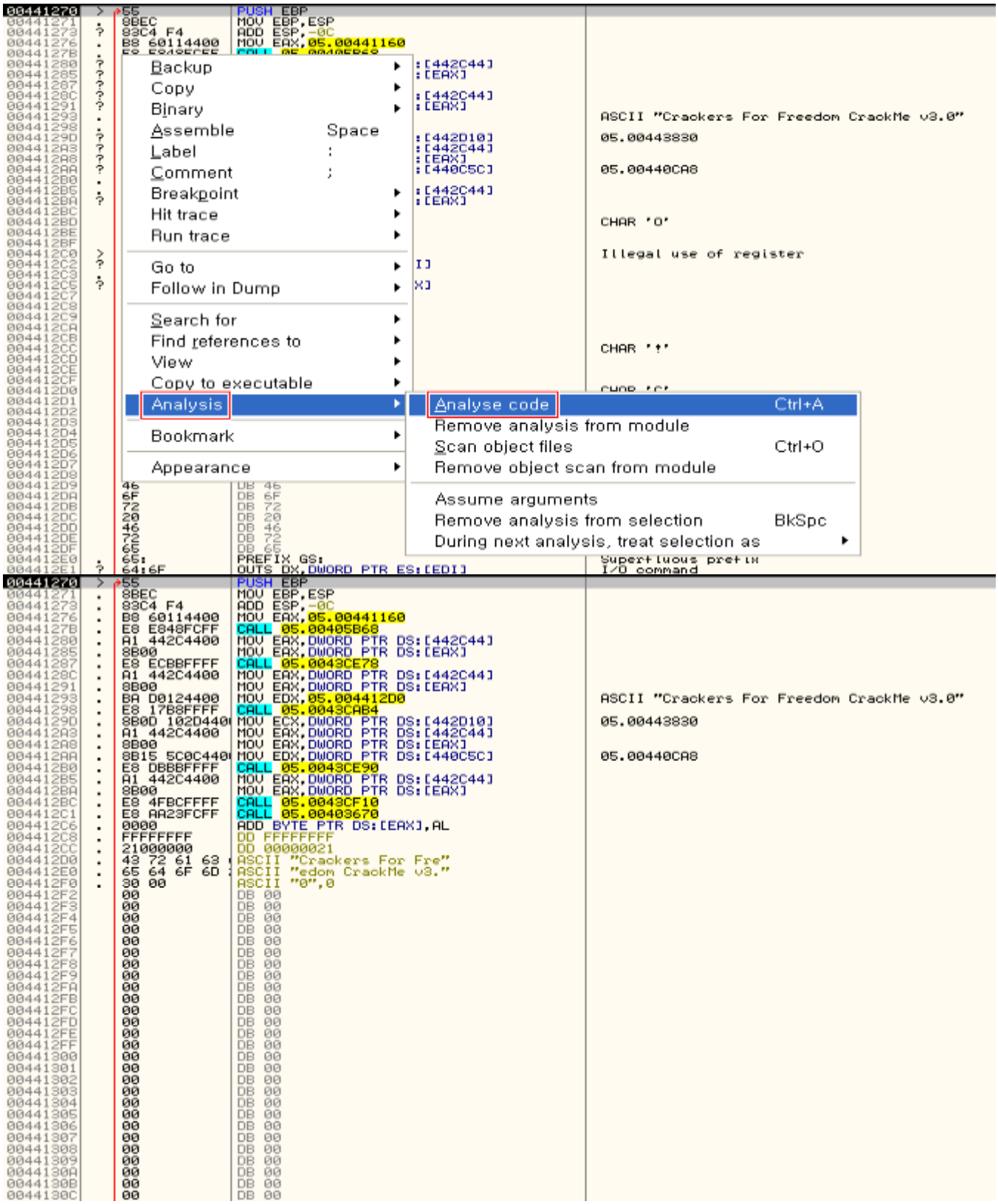
이 명령어의 내부로 진입하면 현재 본 소스로 돌아갈 수 있습니다.

[F4] -> [F7]

```
00441270  >  55            PUSH EBP
00441271  .  8BEC          MOV EBP,ESP
00441273  ?  83C4 F4       ADD ESP,-0C
00441276  .  B8 60114400   MOV EAX,05.00441160
0044127B  .  E8 E848FCFF   CALL 05.00405B68
00441280  ?  A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
00441285  ?  8B00          MOV EAX,DWORD PTR DS:[EAX]
00441287  ?  E8 ECBBFFFF   CALL 05.0043CE78
0044128C  ?  A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
00441291  ?  8B00          MOV EAX,DWORD PTR DS:[EAX]
00441293  .  BA D0124400   MOV EDX,05.004412D0                ASCII "Crackers For Freedom CrackMe v3.0"
00441298  .  E8 17B8FFFF   CALL 05.0043CAB4
0044129D  ?  8B0D 102D440( MOV ECX,DWORD PTR DS:[442D10]     05.00443830
004412A3  ?  A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
004412A8  ?  8B00          MOV EAX,DWORD PTR DS:[EAX]
004412AA  ?  8B15 5C0C440( MOV EDX,DWORD PTR DS:[440C5C]     05.00440CA8
004412B0  .  E8 DBBBFFFF   CALL 05.0043CE90
004412B5  .  A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
004412BA  ?  8B00          MOV EAX,DWORD PTR DS:[EAX]
004412BC     E8            DB E8
004412BD     4F            DB 4F                           CHAR 'O'
004412BE     BC            DB BC
004412BF     FF            DB FF
004412C0  >  FFE8          JMP FAR EAX                     Illegal use of register
004412C2  ?  AA            STOS BYTE PTR ES:[EDI]
004412C3  .  23FC          AND EDI,ESP
004412C5  ?  FF00          INC DWORD PTR DS:[EAX]
004412C7     00            DB 00
004412C8     FF            DB FF
004412C9     FF            DB FF
004412CA     FF            DB FF
004412CB     FF            DB FF
004412CC     21            DB 21                           CHAR '!'
004412CD     00            DB 00
004412CE     00            DB 00
004412CF     00            DB 00
004412D0     43            DB 43                           CHAR 'C'
004412D1     72            DB 72                           CHAR 'r'
004412D2     61            DB 61                           CHAR 'a'
004412D3     63            DB 63                           CHAR 'c'
004412D4     6B            DB 6B                           CHAR 'k'
004412D5     65            DB 65                           CHAR 'e'
004412D6     72            DB 72                           CHAR 'r'
004412D7     73            DB 73                           CHAR 's'
004412D8     20            DB 20                           CHAR ' '
004412D9     46            DB 46                           CHAR 'F'
004412DA     6F            DB 6F                           CHAR 'o'
004412DB     72            DB 72                           CHAR 'r'
004412DC     20            DB 20                           CHAR ' '
004412DD     46            DB 46                           CHAR 'F'
004412DE     72            DB 72                           CHAR 'r'
004412DF     65            DB 65                           CHAR 'e'
004412E0  .  65:           PREFIX GS:                      Superfluous prefix
004412E1  ?  64:6F         OUTS DX,DWORD PTR ES:[EDI]      I/O command
```

이렇게 점프 해왔습니다.

하지만 아직 완전히 복구된 소스는 아닙니다.



이렇게 본 소스로 볼 수 있습니다.

```
Address  Disassembly                              Text string
00440E15 ASCII "Label7"
00440E22 ASCII "Label8"
00440E2F ASCII "Bevel1"
00440E3C ASCII "Label9"
00440E4B ASCII "SpeedButton1Clic"
00440E5B ASCII "k"
00440E63 ASCII "SpeedButton2Clic"
00440E73 ASCII "k"
00440E75 ASCII "TForm1"
00440E96 ASCII "TForm1"
00440E9C DD 05.00440CA8                           ASCII "4wB"
00440EA7 ASCII "Unit1"
00440EDC MOV ECX,05.00440FC8                      ASCII "No Name entered"
00440EE1 MOV EDX,05.00440FD8                      ASCII "Enter a Name!"
00440F08 MOV ECX,05.00440FE8                      ASCII "No Serial entered"
00440F0D MOV EDX,05.00440FFC                      ASCII "Enter a Serial!"
00440F2F MOV EDX,05.00441014                      ASCII "Registered User"
00440F4C MOV EDX,05.0044102C                      ASCII "GFX-754-IER-954"
00440F5A MOV ECX,05.0044103C                      ASCII "CrackMe cracked successfully"
00440F5F MOV EDX,05.0044105C                      ASCII "Congrats! You cracked this CrackMe!"
00440F74 MOV ECX,05.00441080                      ASCII "Beggar off!"
00440F79 MOV EDX,05.0044108C                      ASCII "Wrong Serial,try again!"
00440F8E MOV ECX,05.00441080                      ASCII "Beggar off!"
00440F93 MOV EDX,05.0044108C                      ASCII "Wrong Serial,try again!"
00440FC8 ASCII "No Name entered",0
00440FD8 ASCII "Enter a Name!",0
00440FE8 ASCII "No Serial entere"
00440FF8 ASCII "d",0
00440FFC ASCII "Enter a Serial!",0
00441014 ASCII "Registered User",0
0044102C ASCII "GFX-754-IER-954",0
0044103C ASCII "CrackMe cracked "
0044104C ASCII "successfully",0
0044105C ASCII "Congrats! You cr"
0044106C ASCII "acked this Crack"
0044107C ASCII "Me!",0
00441080 ASCII "Beggar off!",0
0044108C ASCII "Wrong Serial,try"
0044109C ASCII " again!",0
004410A9 MOV ECX,05.004410C8                      ASCII "Have a nice day"
004410AE MOV EDX,05.004410D8                      ASCII "Mail Name/Serial to acidbytes@gmx.net !"
004410C8 ASCII "Have a nice day",0
004410D8 ASCII "Mail Name/Serial"
004410E8 ASCII " to acidbytes@gm"
004410F8 ASCII "x.net !",0
00441169 ASCII "[@",0
004411E5 ASCII " C",0
00441270 PUSH EBP                                 (Initial CPU selection)
00441293 MOV EDX,05.004412D0                      ASCII "Crackers For Freedom CrackMe v3.0"
004412D0 ASCII "Crackers For Fre"
004412E0 ASCII "edom CrackMe v3."
004412F0 ASCII "0",0
00442020 ASCII "Runtime error    "
```

그 후 String 값을 추출해보면 다음과 같이 잘 보입니다.

딱봐도 문제에서 넣어야 할 Key 값들이 보이네요 ^^;

이렇게 성공 메시지을 잘 띄어 줍니다.