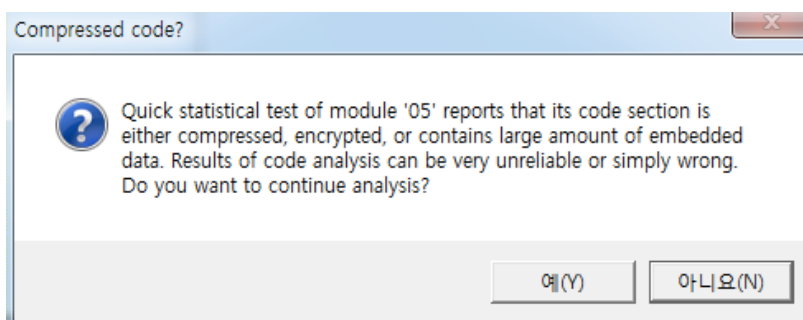


프로그램을 처음 실행한 화면입니다.

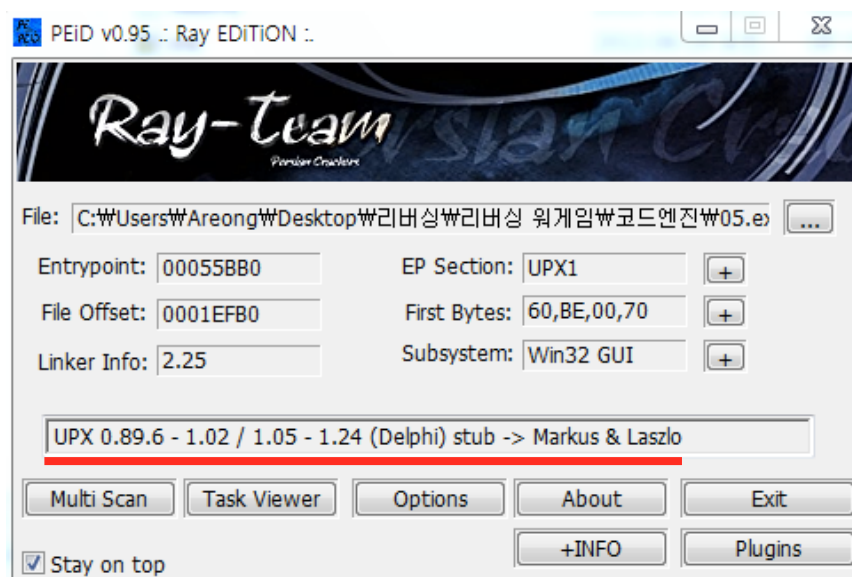
텍스트 박스가 두 개 보이는데 위에는 name이고 아래는 등록키입니다.



키값을 찾으라고 했으니 올리디버거로 실행해 봤는데 이런 메세지 박스가 뜹니다.

해석해보면 암호화가 되어있어 분석결과가 이상할 수 있는데 계속 할꺼냐? 라는 뜻으로 아니요를 누르겠습니다.

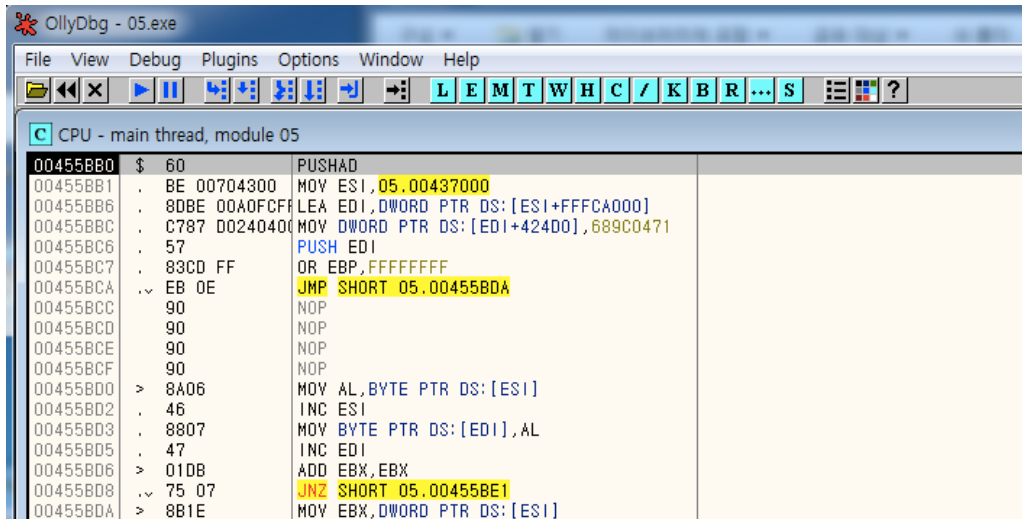
암호화가 되었다는 건 패킹인 것 같군요



PEID란 틀은 파일이 어떤 언어로 만들었는지, 패킹이 되어 있는지 등을 알려주는 유용한 툴입니다.

보면 UPX로 패킹 되어있음을 알 수 있습니다.

다시 올리 디버거로 돌아와서 분석을 시작해보겠습니다.



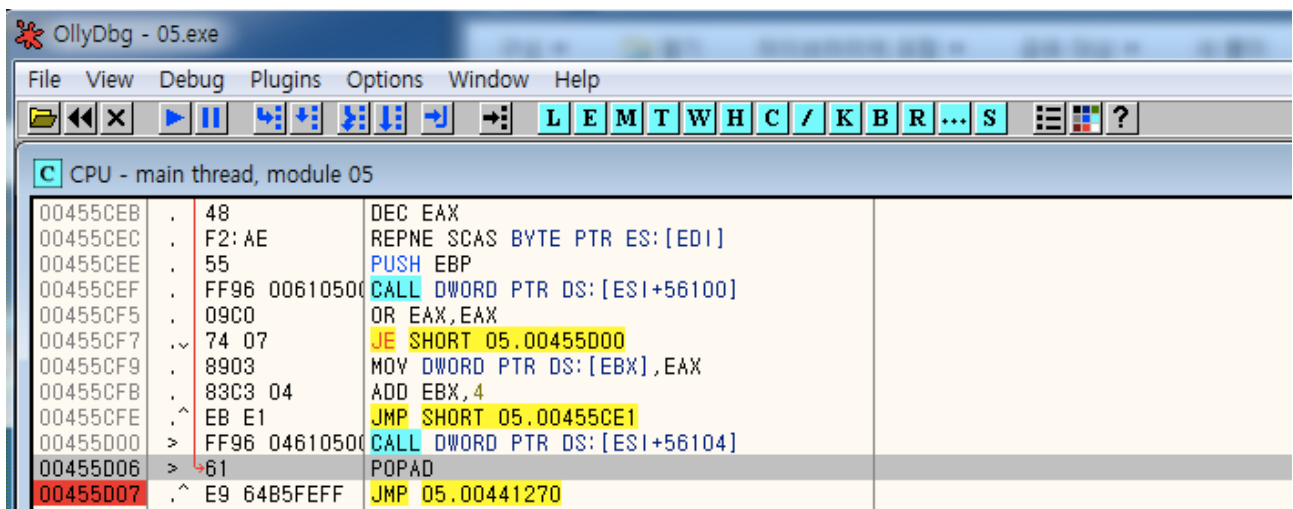
```
OllyDbg - 05.exe
File View Debug Plugins Options Window Help
[Icons] [L] [E] [M] [T] [W] [H] [C] / [K] [B] [R] ... [S] [Icons] [?]

CPU - main thread, module 05
00455BB0 $ 60 PUSHAD
00455BB1 . BE 00704300 MOV ESI,05.00437000
00455BB6 . 8DBE 00A0FCFF LEA EDI,DWORD PTR DS:[ESI+FFFC000]
00455BBC . C787 00240400 MOV DWORD PTR DS:[EDI+42400],689C0471
00455BC6 . 57 PUSH EDI
00455BC7 . 83CD FF OR EBP,FFFFFFFF
00455BCA . 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 > 010B ADD EBX,EBX
00455BD8 . 75 07 JNZ SHORT 05.00455BE1
00455BDA > 8B1E MOV EBX,DWORD PTR DS:[ESI]
```

처음을 보면 PUSHAD라고 되어있는 것을 볼 수 있습니다.

이는 UPX패킹 된 프로그램에서 볼 수 있는 특징입니다.

패킹 된 프로그램은 언패킹을 한 후에 디버깅하는 게 편하지만 그냥 하도록 하겠습니다.



```
OllyDbg - 05.exe
File View Debug Plugins Options Window Help
[Icons] [L] [E] [M] [T] [W] [H] [C] / [K] [B] [R] ... [S] [Icons] [?]

CPU - main thread, module 05
00455CEB . 48 DEC EAX
00455CEC . F2: AE REPNE SCAS BYTE PTR ES:[EDI]
00455CEE . 55 PUSH EBP
00455CEF . FF96 00610500 CALL DWORD PTR DS:[ESI+56100]
00455CF5 . 09C0 OR EAX,EAX
00455CF7 . 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 04610500 CALL DWORD PTR DS:[ESI+56104]
00455D06 > 61 POPAD
00455D07 . E9 6485FEFF JMP 05.00441270
```

밑으로 가다보면 POPAD라고 되어있고 JMP문으로 어디론가 이동하는 것을 알 수 있습니다.

JMP문으로 이동하는 곳이 바로 진짜 프로그램의 시작부분입니다.

OllyDbg - 05.exe

File View Debug Plugins Options Window Help

00441270 > 55 PUSH EBP

00441271 . 8BEC MOV EBP, ESP

00441273 . 83C4 F4 ADD ESP, -0C

00441276 . B8 60114400 MOV EAX, 05.00441160

00441278 . E8 E848FCFF CALL 05.00405868

00441280 . A1 442C4400 MOV EAX, DWORD PTR DS:[442C44]

00441285 . 8B00 MOV EAX, DWORD PTR DS:[EAX]

00441287 . E8 ECB8FFFF 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, 05.00441200 ASCII "Crackers For Freedom CrackMe v3.0"

00441298 . E8 1788FFFF CALL 05.0043CAB4

0044129D . 8B00 102D4400 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 5C0C4400 MOV EDX, DWORD PTR DS:[440C5C] 05.00440CA8

004412B0 . E8 DB88FFFF CALL 05.0043CE90

004412B5 . A1 442C4400 MOV EAX, DWORD PTR DS:[442C44]

004412BA . 8B00 MOV EAX, DWORD PTR DS:[EAX]

004412BC . E8 4F8CFFFF CALL 05.0043CF10

004412C1 . E8 AA23FCFF CALL 05.00403670

004412C6 . 0000 ADD BYTE PTR DS:[EAX], AL

004412C8 . FFFFFFFF DD FFFFFFFF

004412CC . 21000000 DD 00000021

R Text strings referenced in 05:UPX1

Address	Disassembly	Text string
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!"

실제 시작부분으로 이동한 후 모든 text를 찾아보니 인증과 관련 된 문자열들을 볼 수 있습니다.

OllyDbg - 05.exe

File View Debug Plugins Options Window Help

00440F06 . 6A 00 PUSH 0

00440F08 . B9 E80F4400 MOV ECX, 05.00440FE8

00440F0D . BA FC0F4400 MOV EDX, 05.00440FFC

00440F12 . A1 442C4400 MOV EAX, DWORD PTR DS:[442C44]

00440F17 . 8B00 MOV EAX, DWORD PTR DS:[EAX]

00440F19 . E8 4AC1FFFF CALL 05.0043D068

00440F1E > 8D55 FC LEA EDX, DWORD PTR SS:[EBP-4]

00440F21 . 8B83 C4020000 MOV EAX, DWORD PTR DS:[EBX+2C4]

00440F27 . E8 F4FEFDFE CALL 05.00420E20

00440F2C . 8B45 FC MOV EAX, DWORD PTR SS:[EBP-4]

00440F2F . BA 14104400 MOV EDX, 05.00441014 ASCII "Registered User"

00440F34 . E8 F32BFCFF CALL 05.00403B2C

00440F39 . 75 51 JNZ SHORT 05.00440F8C

00440F3B . 8D55 FC LEA EDX, DWORD PTR SS:[EBP-4]

00440F3E . 8B83 C8020000 MOV EAX, DWORD PTR DS:[EBX+2C8]

00440F44 . E8 D7FEFDFE CALL 05.00420E20

00440F49 . 8B45 FC MOV EAX, DWORD PTR SS:[EBP-4]

00440F4C . BA 2C104400 MOV EDX, 05.0044102C ASCII "GFX-754-IER-954"

00440F51 . E8 D62BFCFF CALL 05.00403B2C

00440F56 . 75 1A JNZ SHORT 05.00440F72

00440F58 . 6A 00 PUSH 0

00440F5A . B9 3C104400 MOV ECX, 05.0044103C

00440F5F . BA 5C104400 MOV EDX, 05.0044105C

ASCII "CrackMe cracked successfully"

ASCII "Congrats! You cracked this CrackMe!"

해당 부분으로 이동해 소스를 분석하니 우선 이름이 빈칸인지 확인하고 빈칸이 아니면 키가 빈칸인지 확인합니다.

둘 다 빈칸이 아니면 그 내용을 비교하는데 위의 사진에 이름과 키의 비교값이 존재합니다.