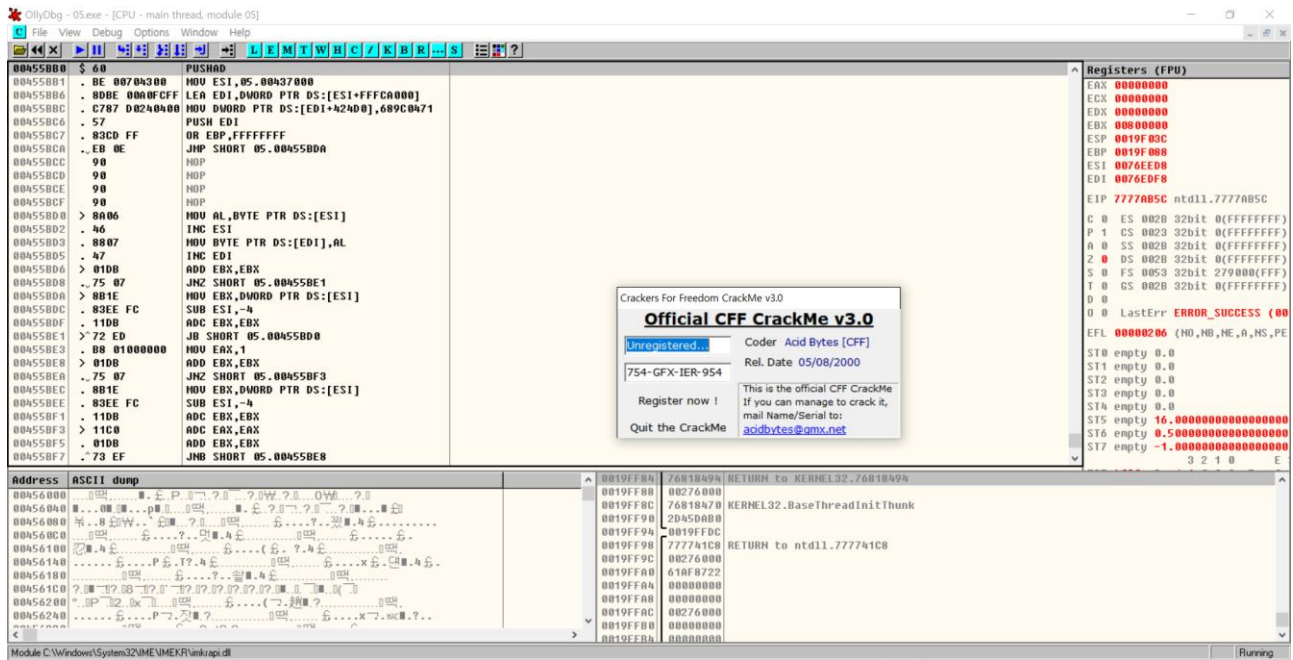

[CodeEngn]

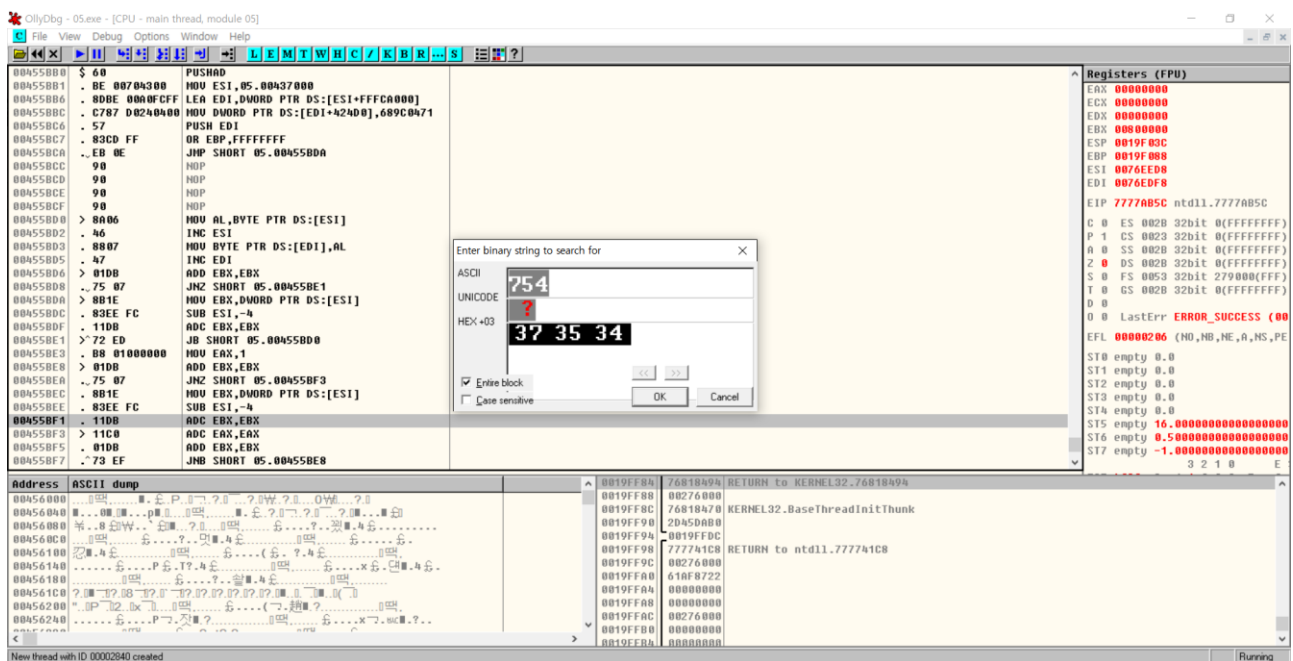
Basic RCE L05

== 언패킹 하지 않고 문제풀이 ==

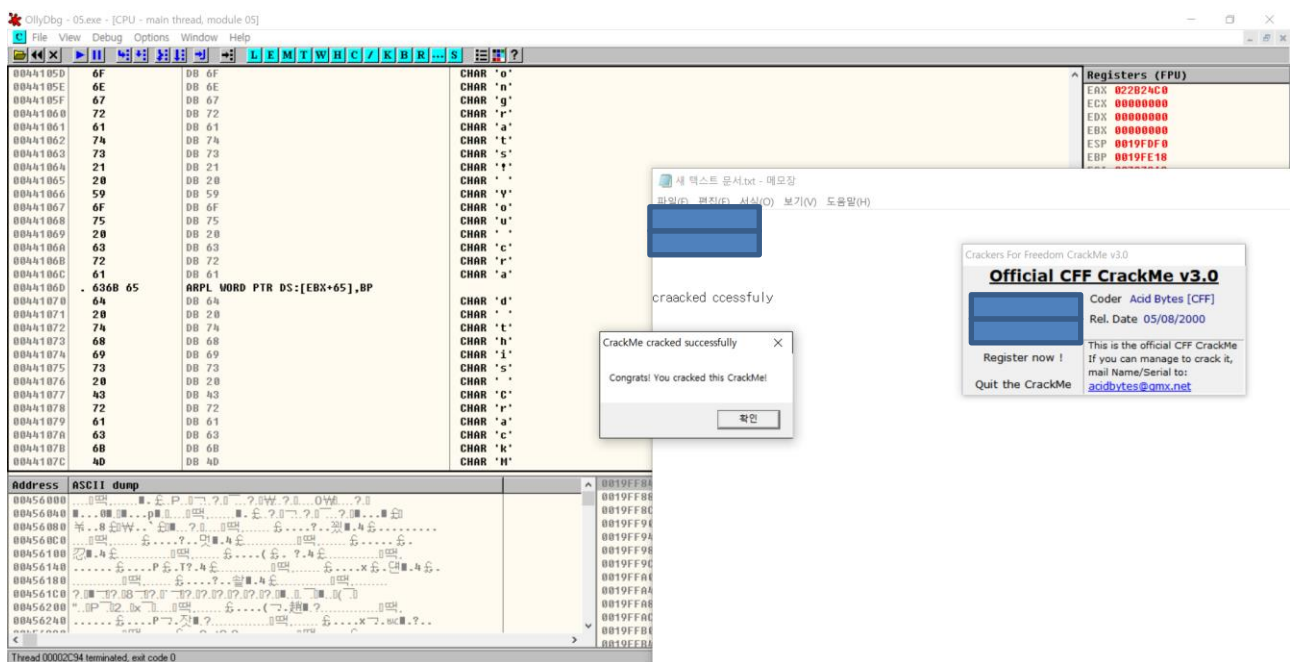
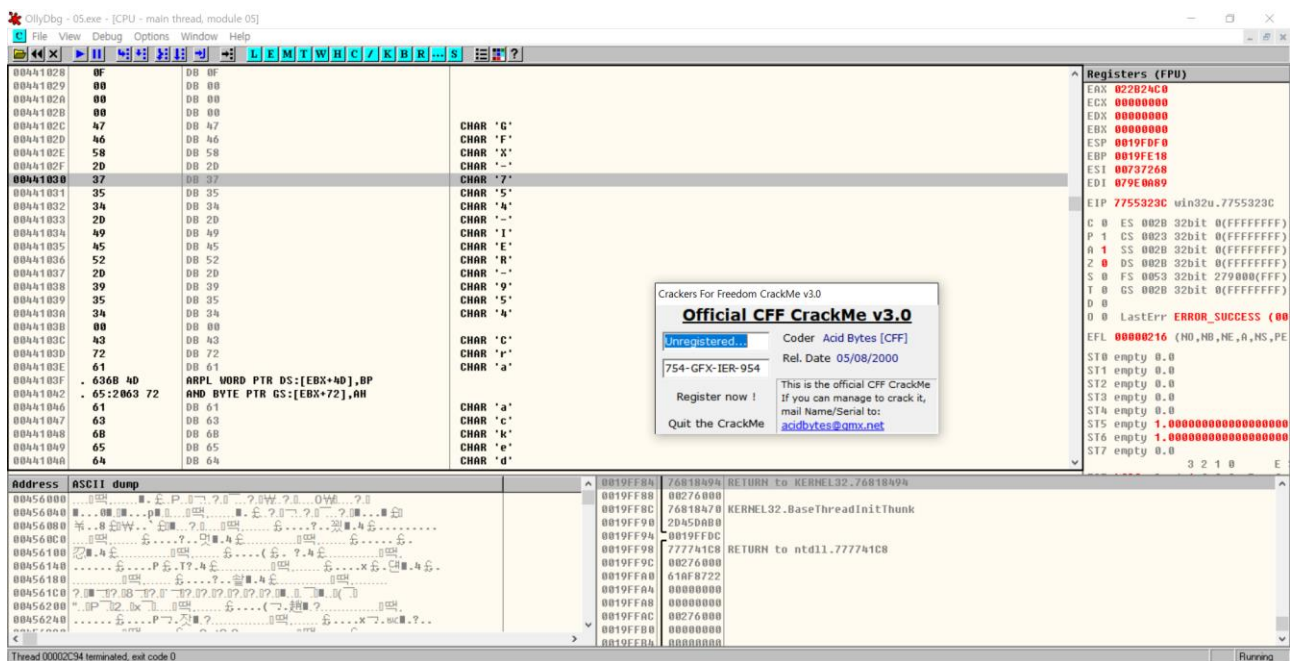


해당 문제를 디버깅하고 있는 장면이다.

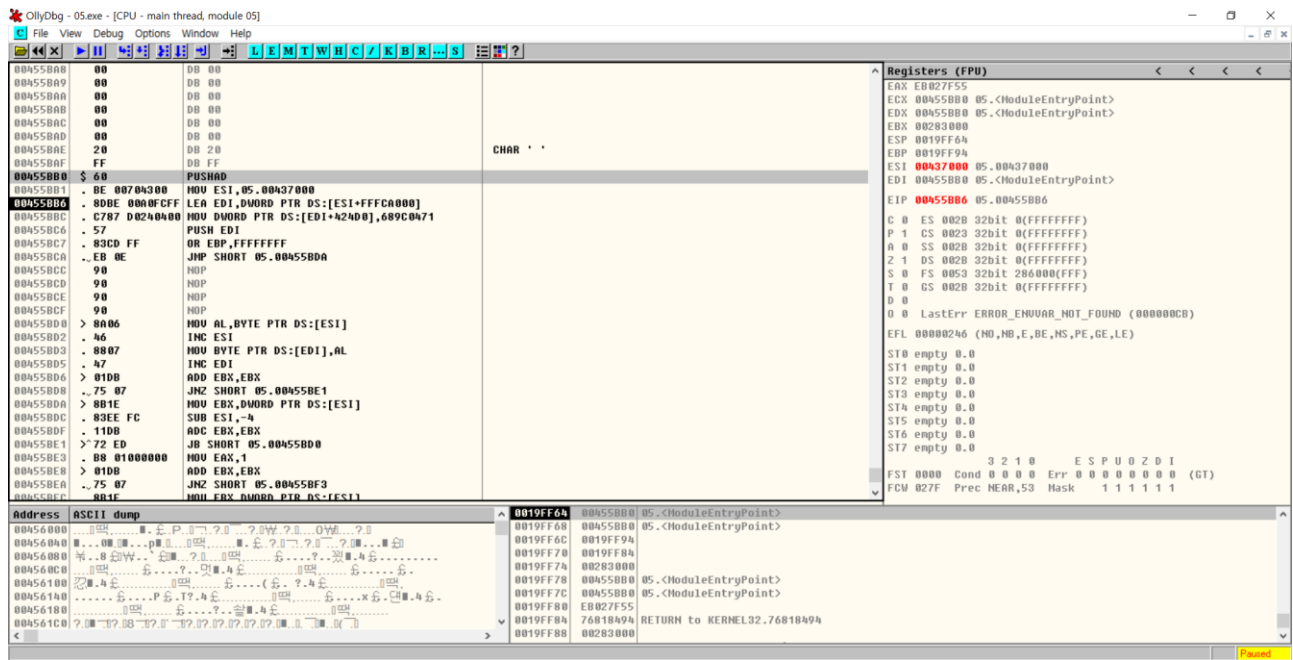
어떻게 접근할까 하다가, 754 라는 숫자가 미리 입력이 되어 있는 것을 알았다.



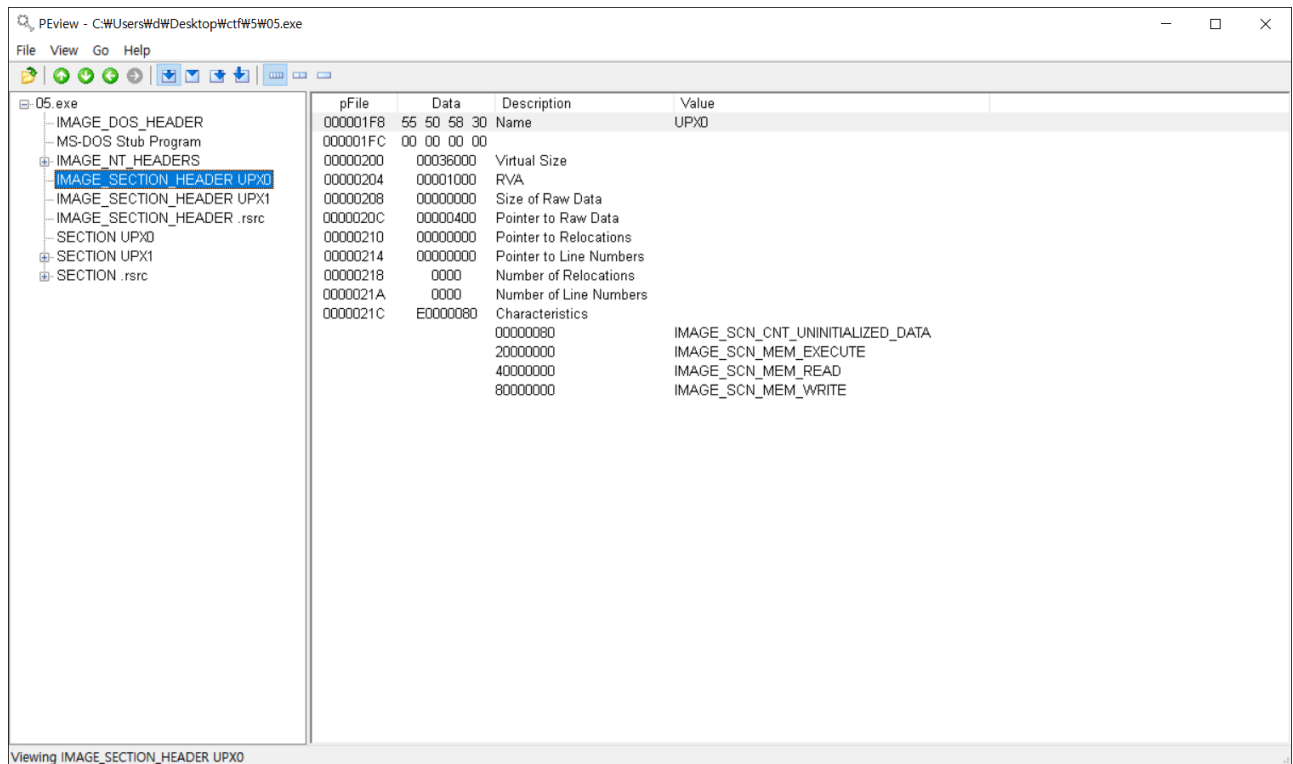
그래서 해당 숫자를 검색해보았다.



== 언패킹 하고 문제풀이 ==



검색을 해보니, PUSHAD 가 있다면, 이 프로그램은 패킹이 되었다는 것을 알 수 있다고 한다.



해당 프로그램은 UPX 로 패킹이 되어 있었다.

```
cmd 명령 프롬프트

upx: 05.exe: AlreadyPackedException: already packed by UPX

Packed 1 file: 0 ok, 1 error.

C:\Users\wd\Desktop\ctf\5>upx.exe 05.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017

File size      Ratio      Format      Name
-----
upx: 05.exe: AlreadyPackedException: already packed by UPX

Packed 1 file: 0 ok, 1 error.

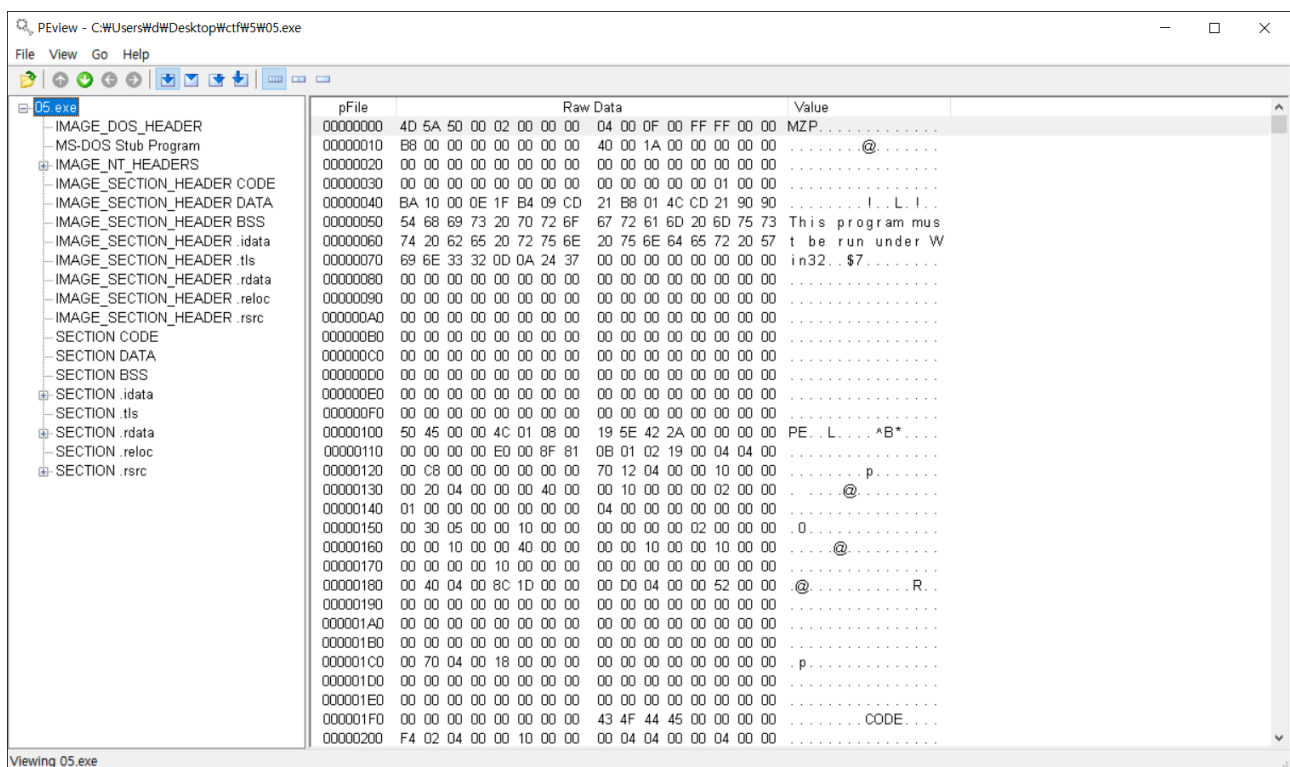
C:\Users\wd\Desktop\ctf\5>upx.exe 05.exe -d -k
Ultimate Packer for executables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017

File size      Ratio      Format      Name
-----
315392 <-    132608    42.05%    win32/pe    05.exe

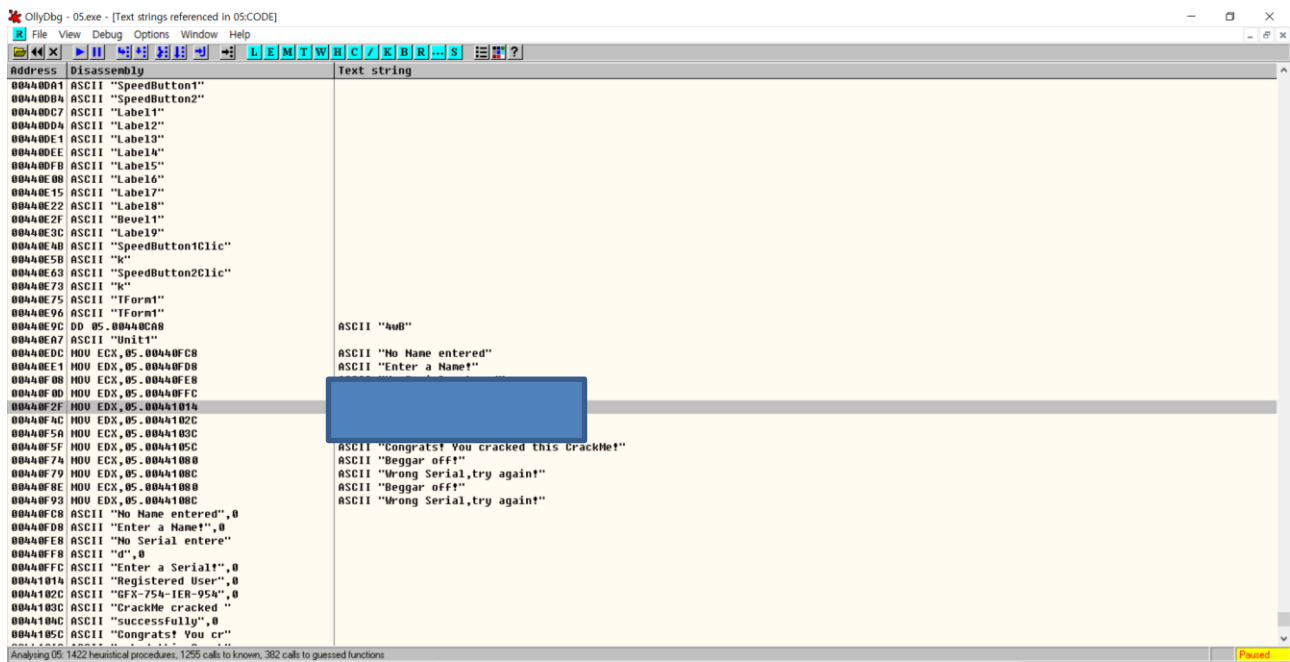
Unpacked 1 file.

C:\Users\wd\Desktop\ctf\5>upx.exe 05.exe -d -k
Ultimate Packer for executables
Copyright (C) 1996 - 2017
```

UPX 언패킹을 한다.



언패킹을 하고 난 뒤에 모습이다.



올리디버거에서 text string 을 봤는데, 정답이 바로 있었다.