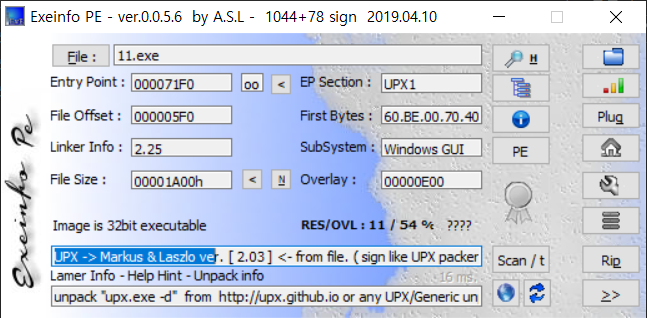
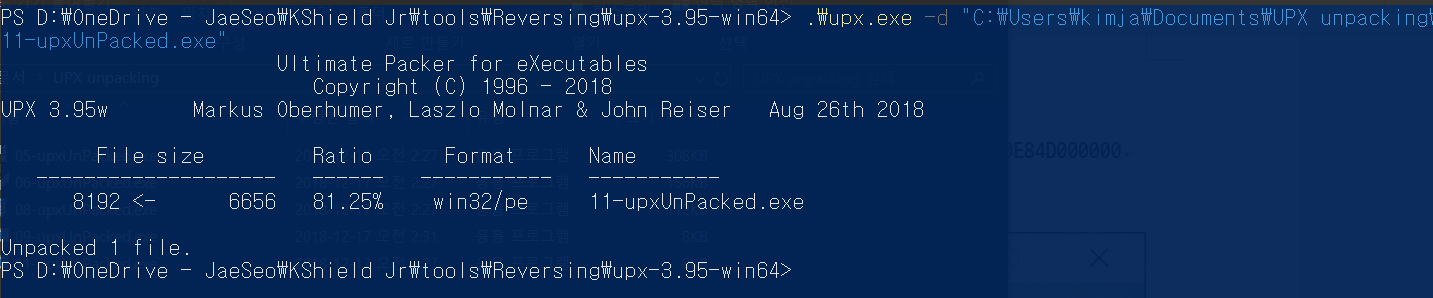
**11.exe -** OEP를 찾으시오. Ex) 00401000 / Stolenbyte 를 찾으시오.

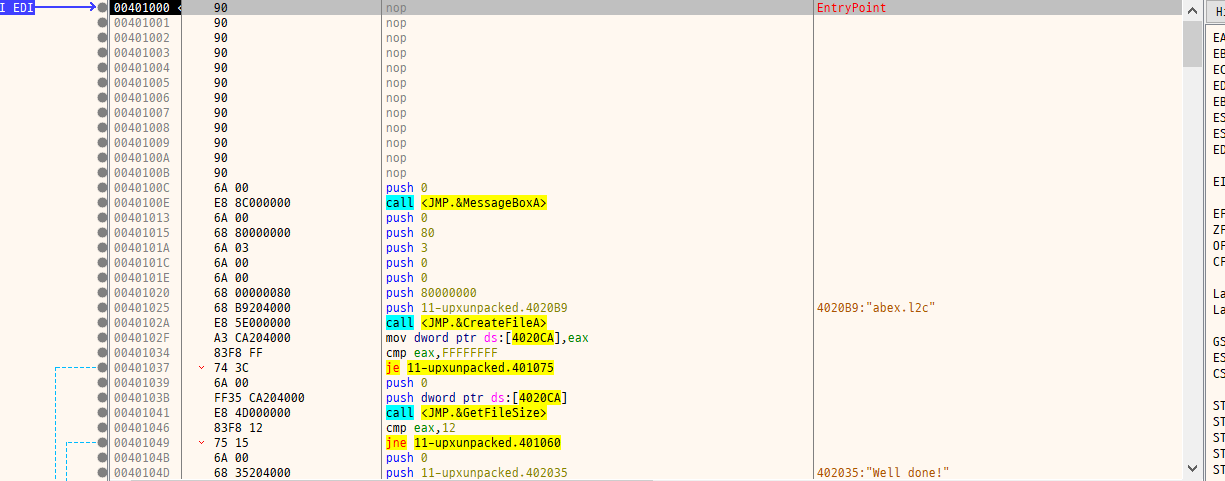
Ex) FF35CA204000E84D000000 정답인증은 OEP+ Stolenbyte Ex) 00401000FF35CA204000E84D000000

프로그램 PE 분석을 일단 진행하여 본다.



UPX로 Packing 되어 있는 것을 알 수가 있는데 UPX로 Unpacking을 진행한다.



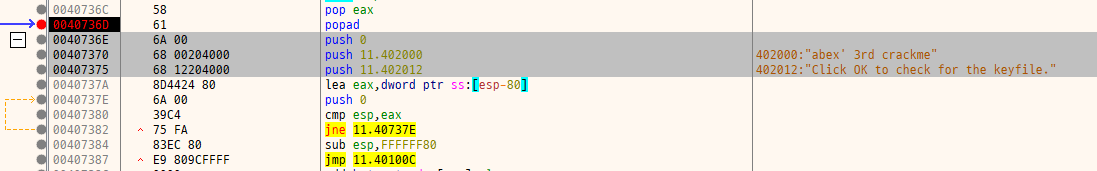


UPX로 Unpacking된 파일을 X32dbg로 열어보니 NOP으로 되어 있는 부분이 있다.

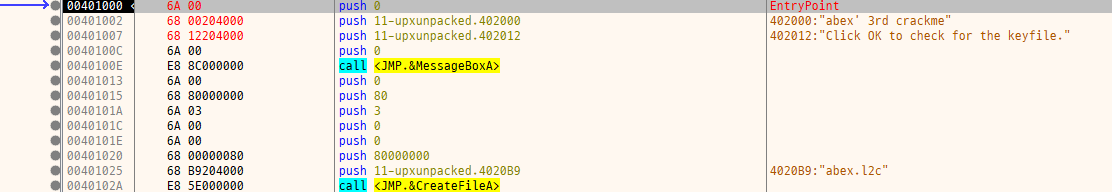
Stolen Byte가 있으니 Packing된 파일을 통해 분석을 해본다.



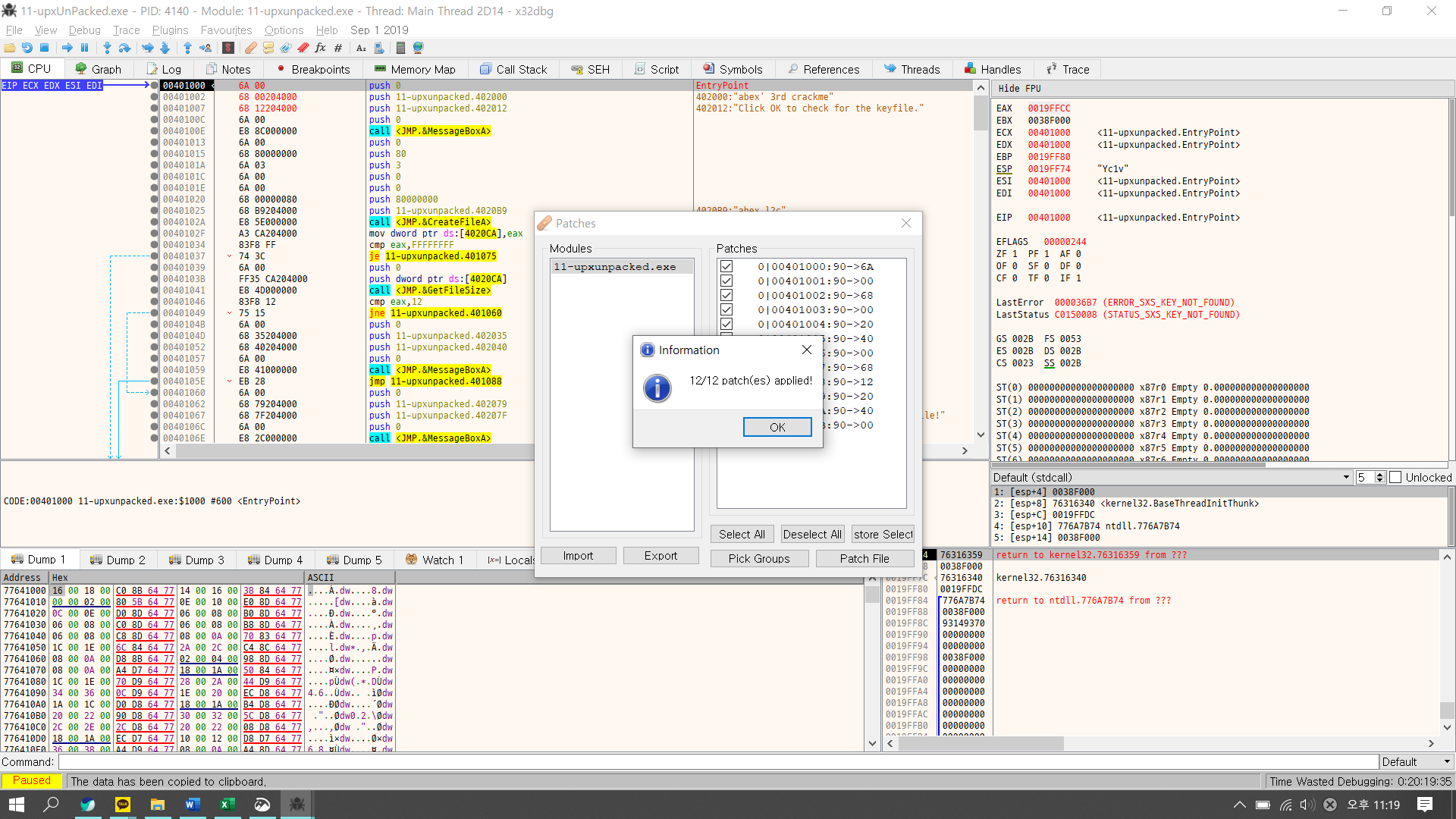
Upx로 unpacking 끝난 이후 POPAD로 레지스터를 복구하는 곳을 찾아 분석한다.



Popad 이후 push를 하는 모습을 볼 수가 있는데 아직 OEP로 들어가기 전에 작동하는 것을 보아 Stolen byte로 추정이 된다. 그리고 JMP 11.40110C로 OEP로 들어가는 모습을 확인할 수 있다.



Unpacking 된 파일 Nop 부분에 Stolen Byte를 집어넣어 정상적인 프로그램으로 바꾼다.



**정답: 004010006A0068002040006812204000**