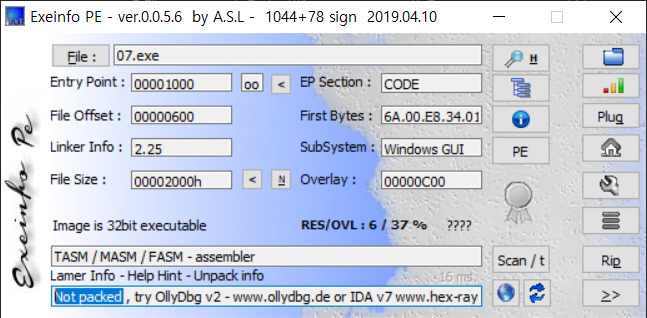
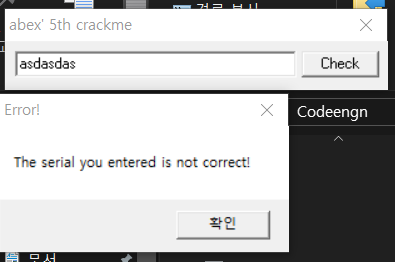
**06.exe -** 컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 'ß어떤것'으로 변경되는가

일단 프로그램을 디버깅 하기 전 PE분석을 해본다.

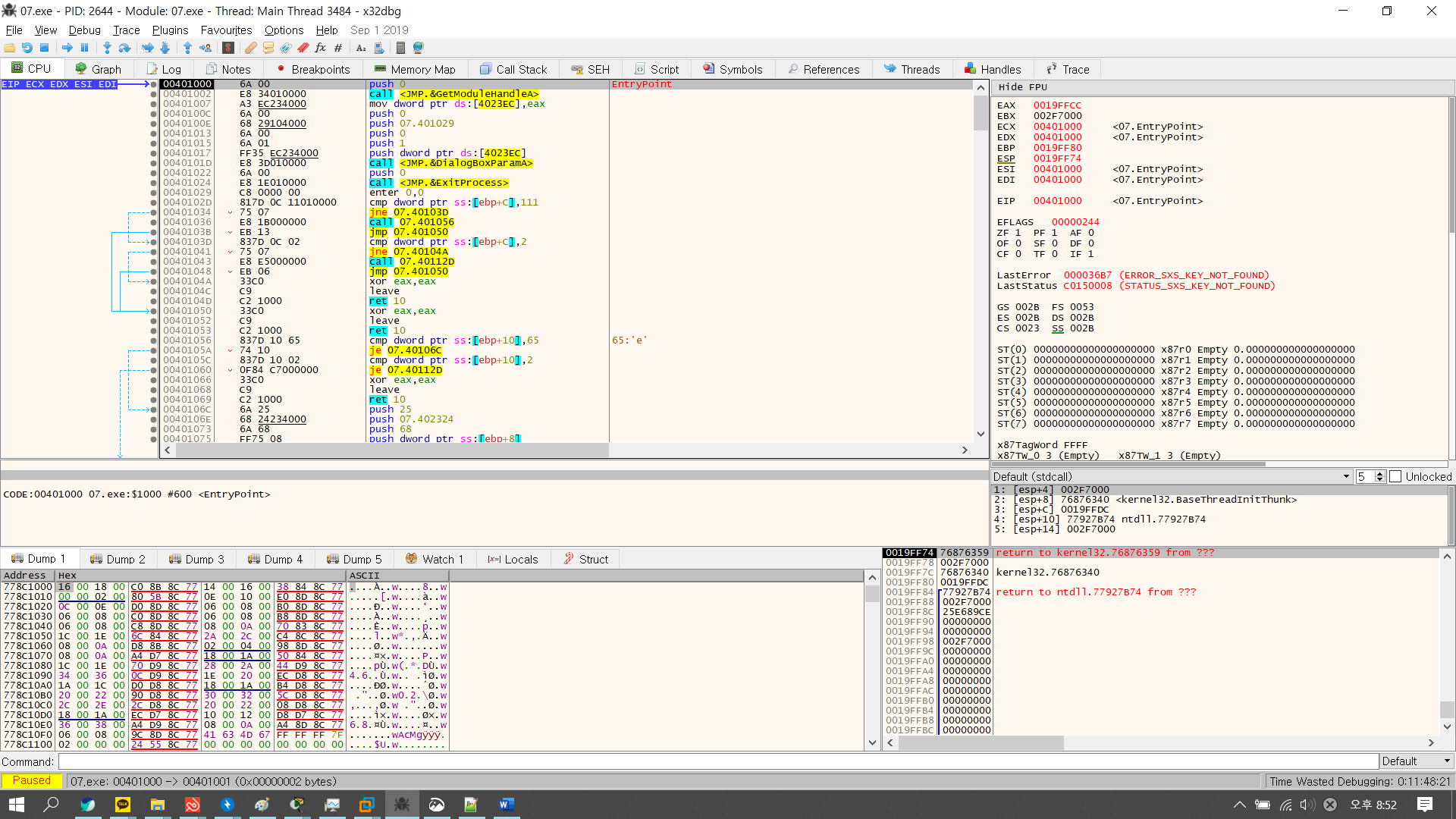


ExeinfoPE를 통해 Not packed가 되었다는 것을 확인함.

****

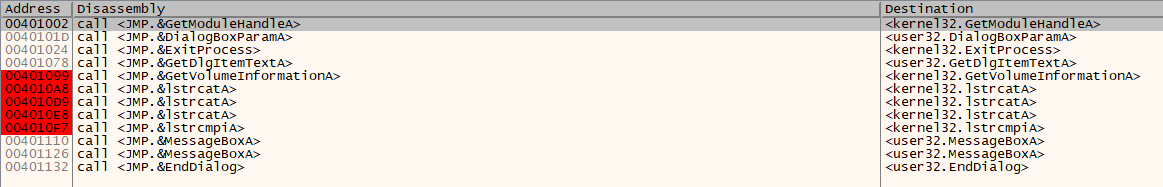
프로그램을 실행시 시리얼 키를 입력 받고 확인을 하는 프로그램으로 추정됨.

X32dbg로 실행하여 분석을 시작한다.

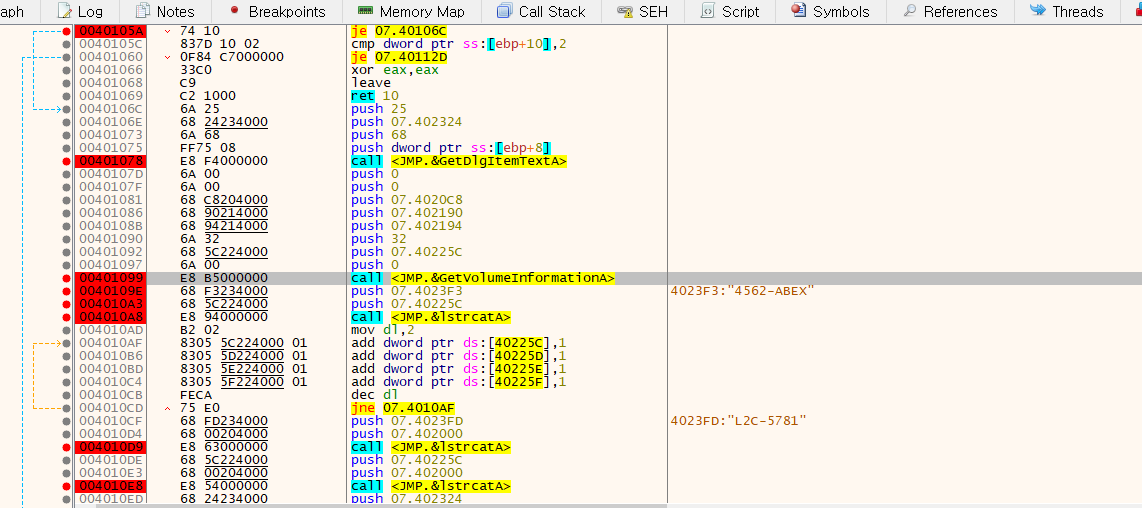


일단 Check 버튼을 눌렀을 때 하드디스크의 이름 정보를 가져오는 함수가 작동될 것으로 예상된다.

이때 keyword(volume, disk, information, get 등)을 가지고 인터럽트를 검색해본다.

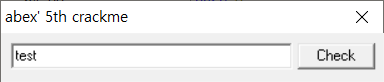


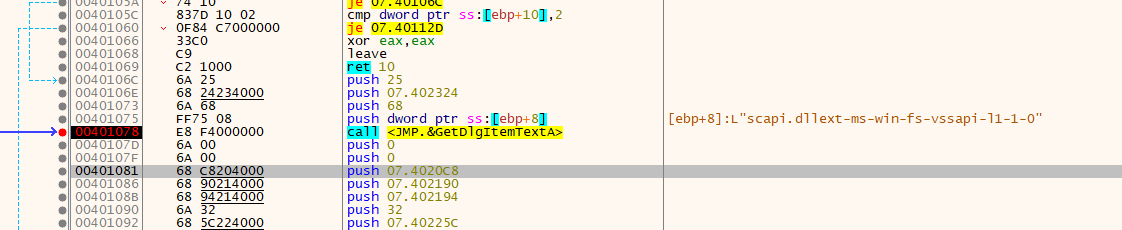
이때 “GetVolumeInformationA” 함수를 발견하게 되는데 이 함수를 통해 볼륨의 이름을 가져오는 것으로 추정이 된다.



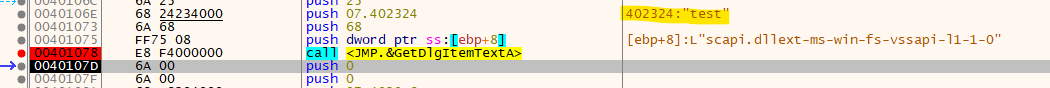
이제 함수를 호출하는 주소로 들어가 보면 위와 같이 inputbox에서 입력 값을 받아오고 어떠한 문자열과 “lstcatA” 함수를 호출하는 것을 볼 수가 있다.

이때 어떠한 작동을 하는지에 대해 분석하기 위해 함수를 호출하는 위치에 Break Point를 걸고 관찰을 한다.

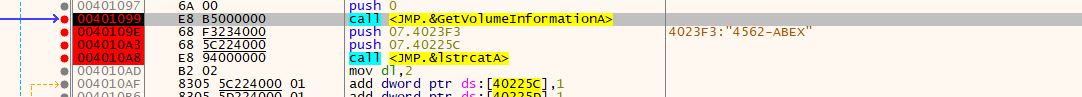




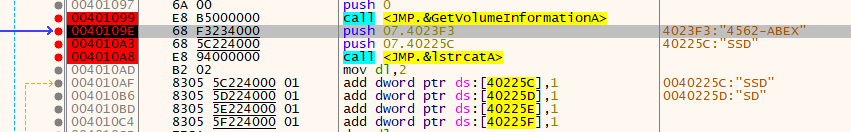
일단 첫번째 Break Point에서 이제 여기서 F8를 눌러 Call를 한다.



실행 결과 402324에 “test” 라는 문자열이 저장된 것을 볼 수 있다.

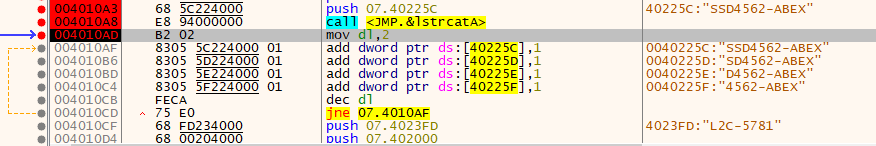


두번째 Break Point에서 F8를 눌러 Call를 하면 어떠한 변화가 생기는지 관찰을 한다.



그 결과 40225C에 저의 하드 볼륨 이름인 SSD가 들어가게 되는 것을 볼 수가 있다.

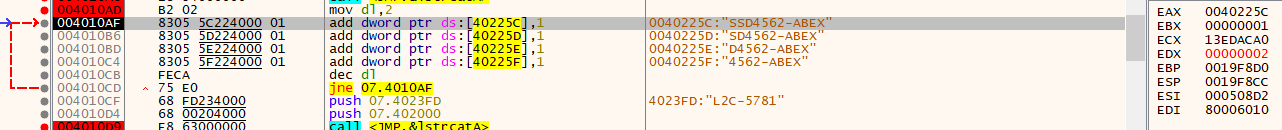
그리고 Call “lstrcatA”라는 함수를 호출하는데 어떠한 변화가 생기는지 관찰을 한다.



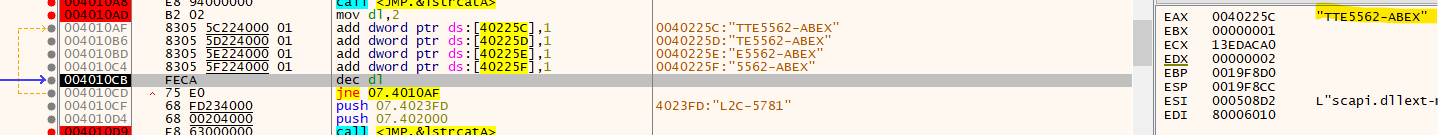
Call를 한 결과 40225C에 시리얼 키로 추정이 되는 문자열과 결합이 되어 “SSD4562-ABEX”가 된 것을 볼 수 있다.

그리고 DL을 2로 설정하고 문자열에 1을 더하는 작업을 여러 번 한 뒤 Dl를 1감소시켜 DL이 0이 될 때 까지 반복을 하고 있는 것을 볼 수 있다.

이제 어떻게 문자열이 변화하는지 관찰을 한다.



일단 DL은 2로 설정이 된 것을 볼 수 있다.



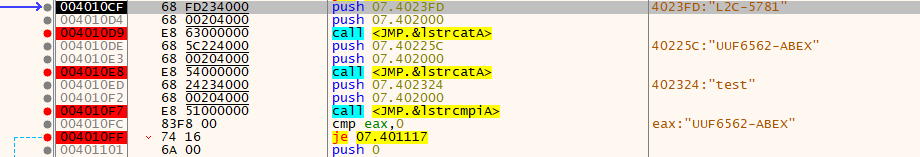
그리고 앞문자부터 하나씩 1씩 증가하는 것을 4번 하여 TTE5562-ABEX가 되는 것을 볼 수 있다.

이제 DL이 0이 되어 반복문이 끝날 때까지 어떻게 변화하는지 관찰하여 본다.

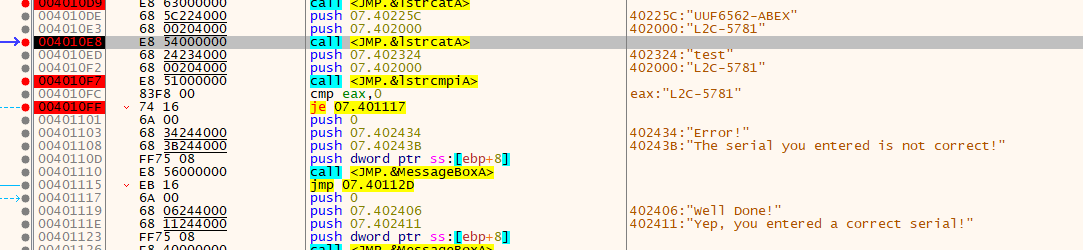


최종적으로 UUF6562-ABEX가 되는 것을 볼 수 있다.

이제 밑에는 있는 부분을 이어서 분석을 해본다.

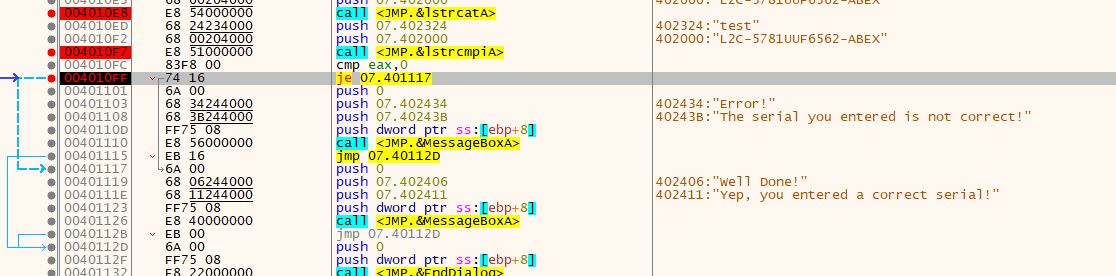


새로운 키조합에 사용되는 것으로 예상이 되는 문자열 L2C-5781를 stack에 올린다.

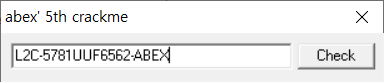


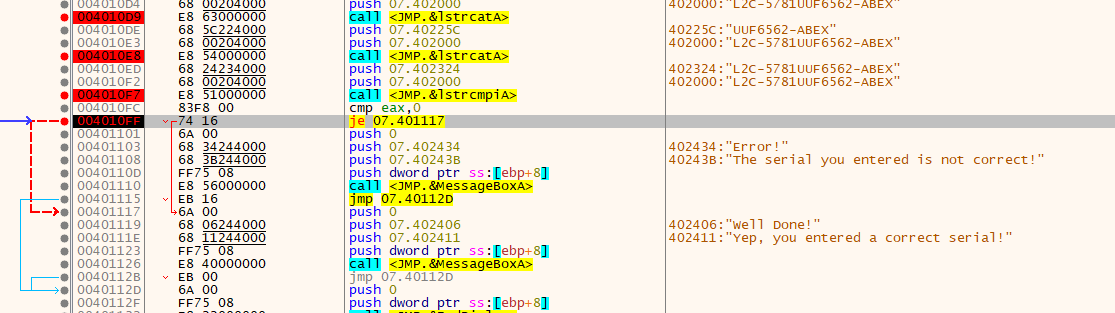
또한 그 이후 “lstrcatA” 함수를 통해 L2C-5781와UUF6562-ABEX를 합치는 것을 볼 수 있다.

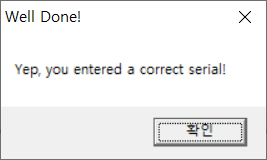
그리고 “lstrcmpiA” 함수를 통해 비교한 결과를 ZF 받고 메시지를 출력하는 것을 볼 수가 있다.



이때 생성된 시리얼키값 생성 알고리즘을 분석한 것이 정확한지 직접 넣어서 확인해본다.







이러한 결과를 토대로 시리얼 키를 생성하는 알고리즘은 드라이브의 볼륨이름을 가져와 4562-ABEX와 결합을 하고 앞 4글자에 1씩더하는 것을 2번 하여서 L2C-5781와 결합하여 최종 시리얼 키를 생성하는 것을 파악할 수 있다.

이제 문제로 돌아와 C드라이브 이름이 CodeEngn일때의 시리얼 키는 “L2C-5781EqfgEngn4562-ABEX” 라는 것을 알 수가 있다. 그리고 CodeEngn은 EgfgEngn으로 변화하는 것을 알 수 있다.

**정답: EgfgEngn**