리얼 라이브 엔진 *Step by Step Manual*
By 마이아크

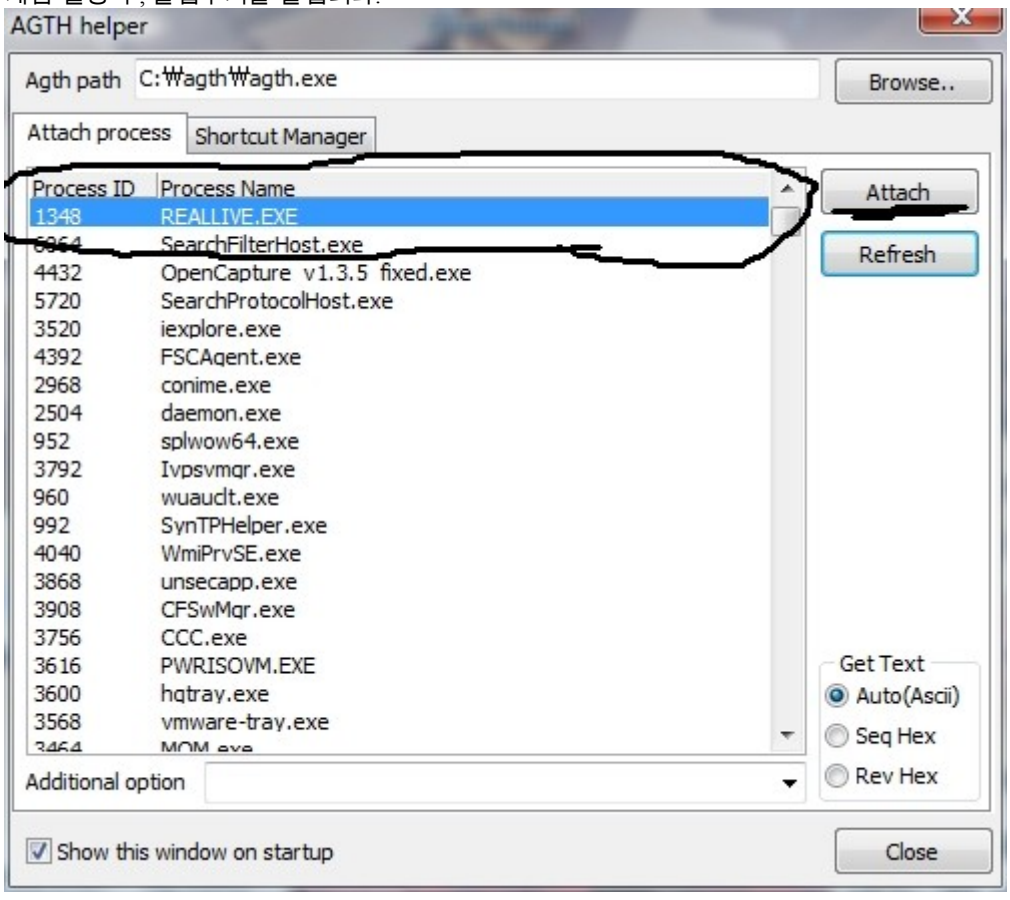
일단 찾는 법 자체는 착한님의 "리얼 라이브 초간편 코드 찾기 메뉴얼" http://www.aralgood.com/zbxe/board_lecture/75386
을 베끼다 싶이 했습니다. 예제만 다르죠.

준비사항:
1. 게임을 설치 할 수 있는 지식.
2. 리얼라이브 엔진 게임을 구별할 수 있는 지식.
3. 어플로케일
4. 최신 아랄트랜스
5. EditPlus2
6. UltraEdit
7. Ollydbg 1.10
8. Cliphooker & 최신 AGTH

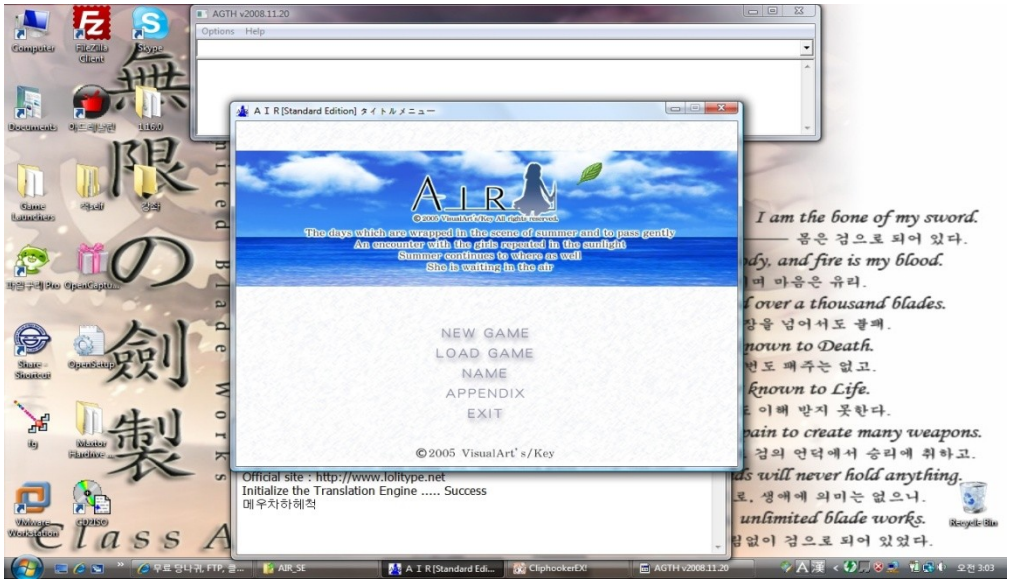
자, 이제 찾아보죠.

예제는 AIR Standard Edition.
게임을 어플로 설치 후, 어플로 실행합니다.

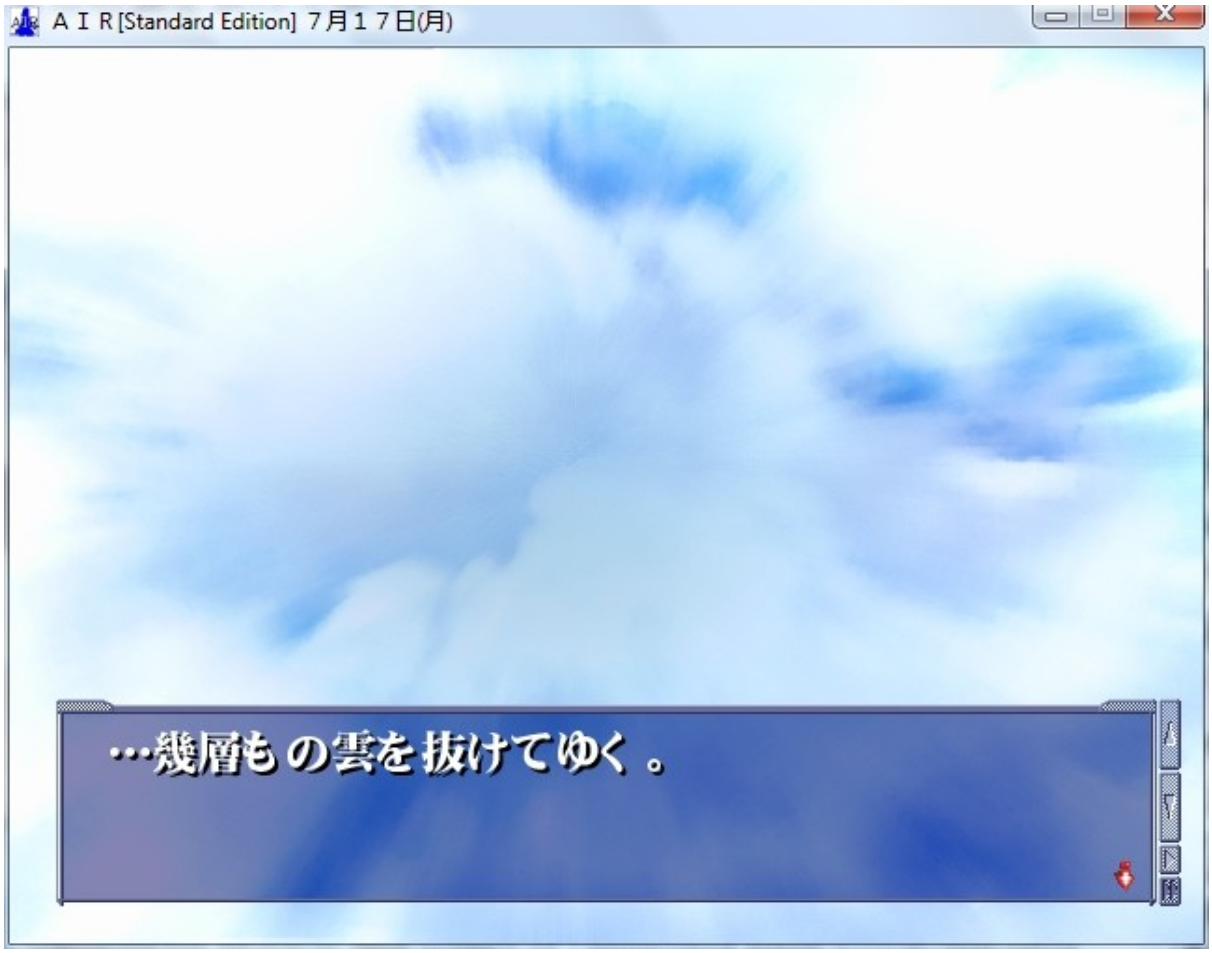
게임 실행 후, 클립후커를 돌립니다.



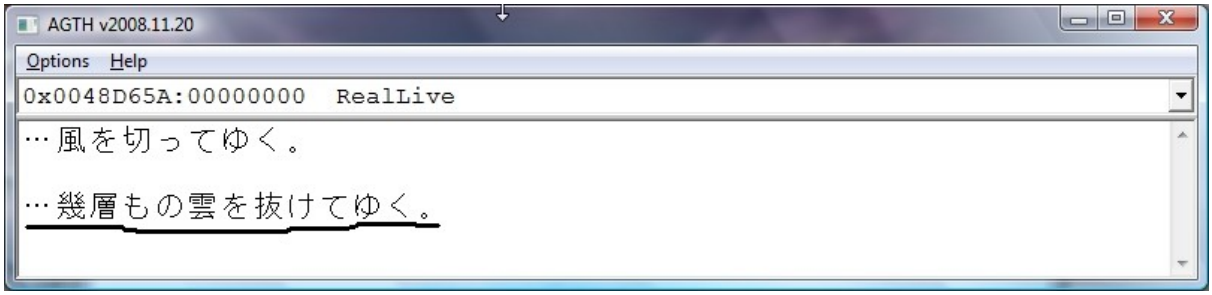
REALLIVE.EXE 가 게임 클릭 후, Attach 버튼을 누르면.....



성공!!!!!
이제 게임을 실행합시다.

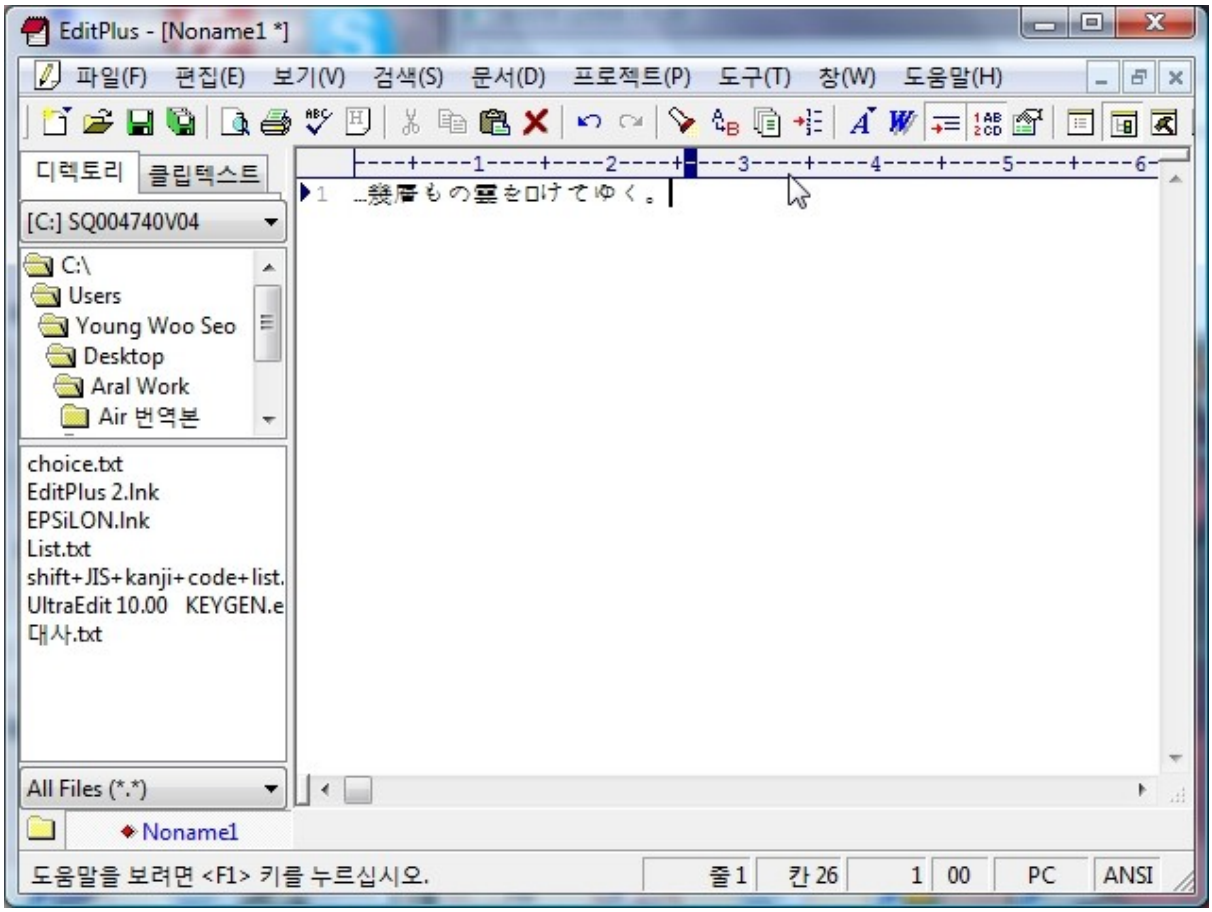


첫번째대사는 됐고....두번째까지 진행합시다. (윗 스샷은 두번째 대사)



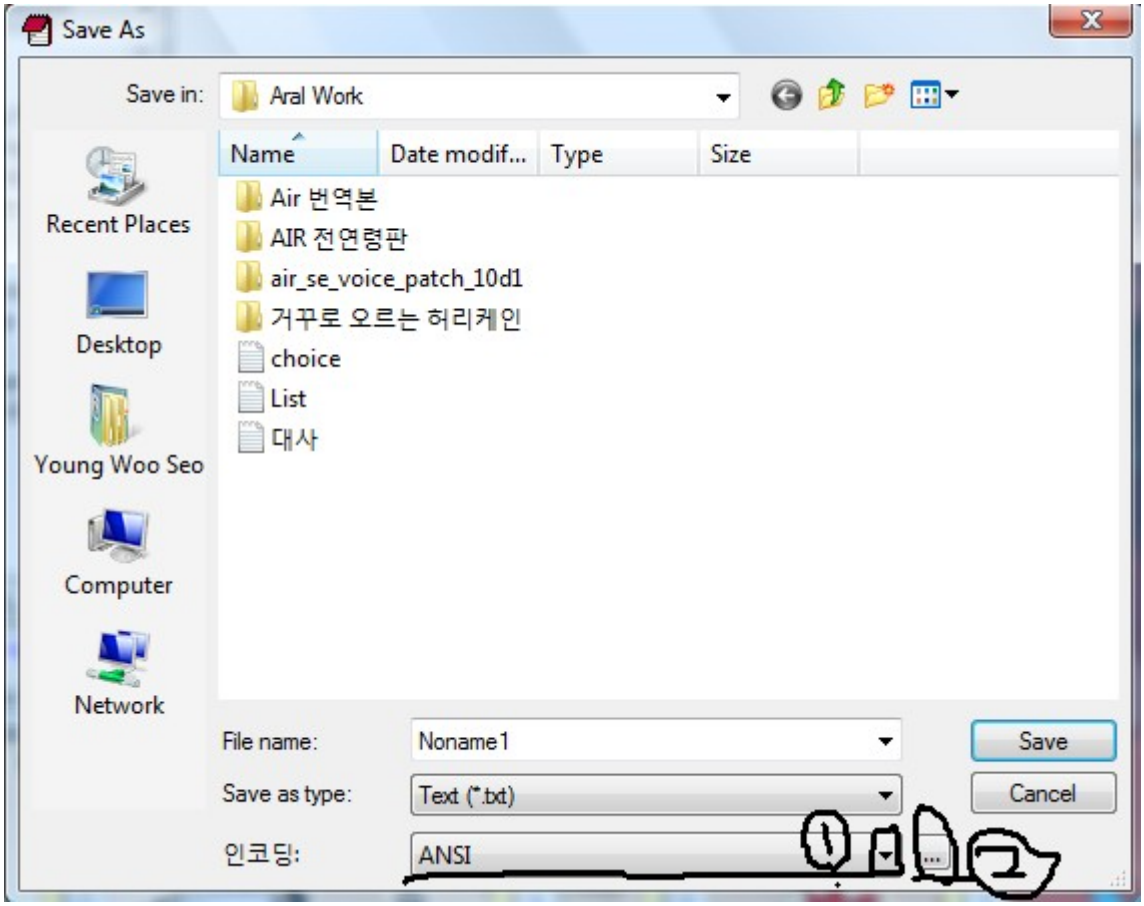
저 두번째 대사를 복사합시다. (CTRL+C)

그리고.....



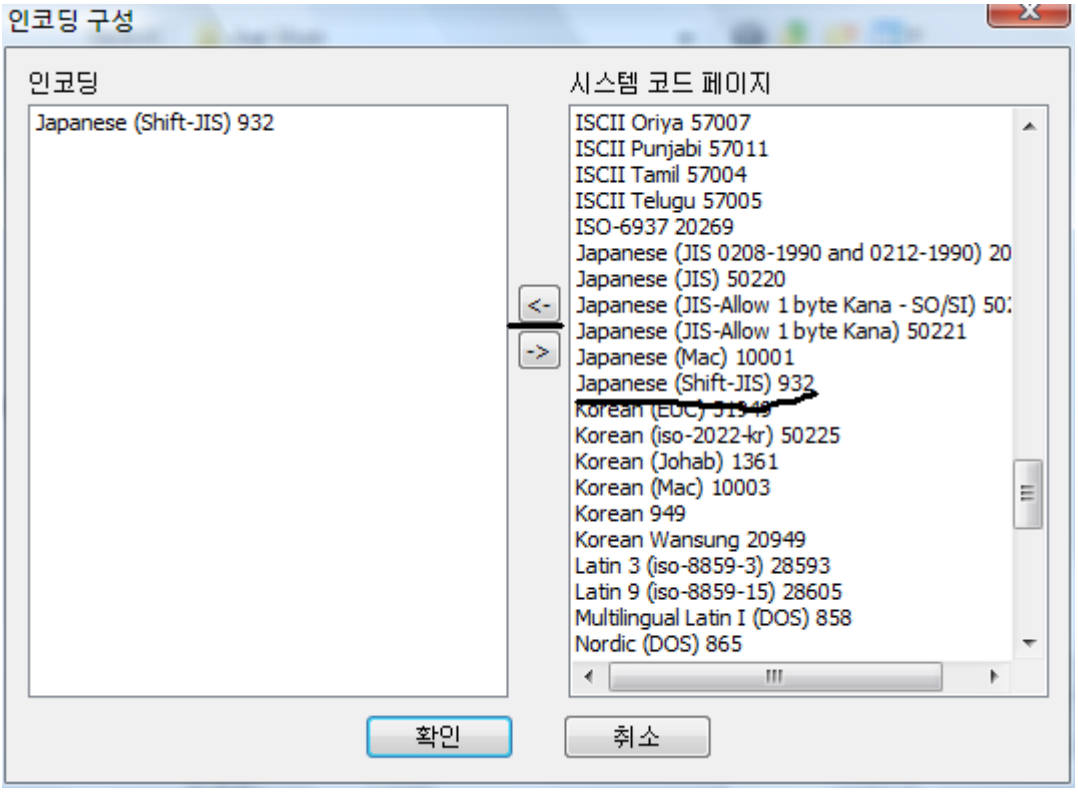
이렇게 붙여넣기를 합시다.

이제 저장을 합시다.



인코딩을 Japanese(Shift-JIS)932 로 바꿔줍시다.

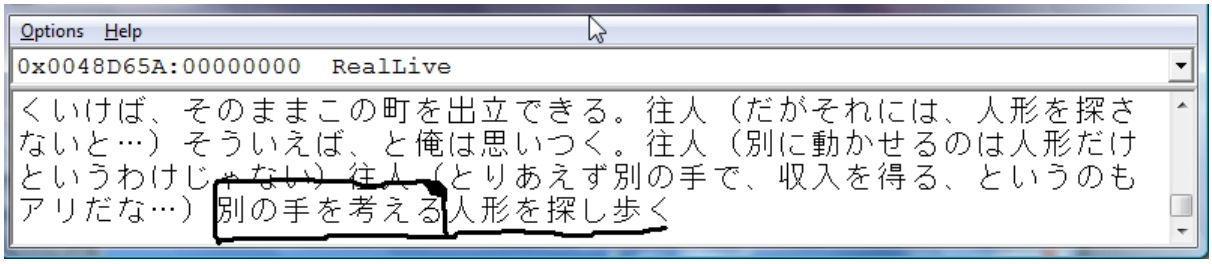
만약에 그러한 인코딩이 없다 하시면 2 번을 눌러주세요 ^ ^



이러한 창이 뜹니다. 스크롤 다운 후, Japanese (Shift-JIS) 932 을 클릭 후 오른쪽으로 옮겨줍시다.

자, 이제 저장합시다.

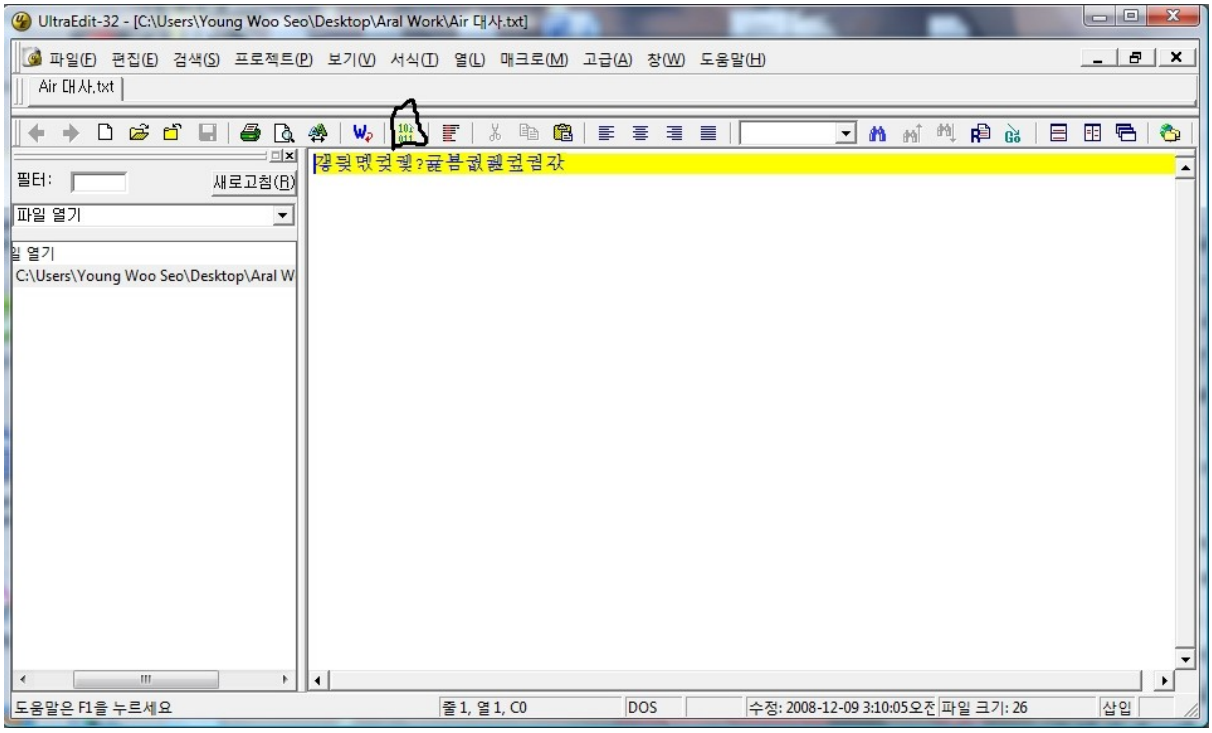
홧김에 선택지까지 수집하죠. 대사와 마찬가지로 이 상태에서 수집합니다.



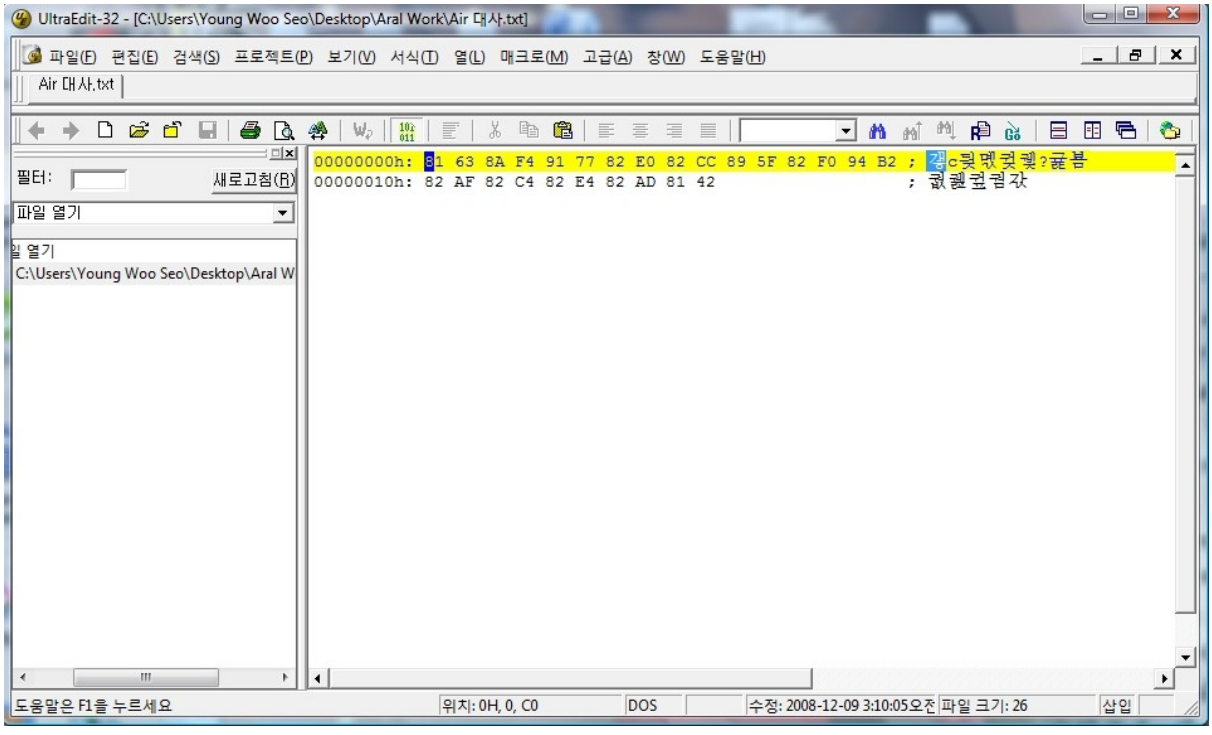
사각형과 밑 줄이 두 개의 선택지 입니다. 첫 번째 선택지만 수집하죠. (AGTH 의 상태가 저런건 CTRL 스킵신공으로 인해..)

대사와 선택지 수집이 끝났습니다.

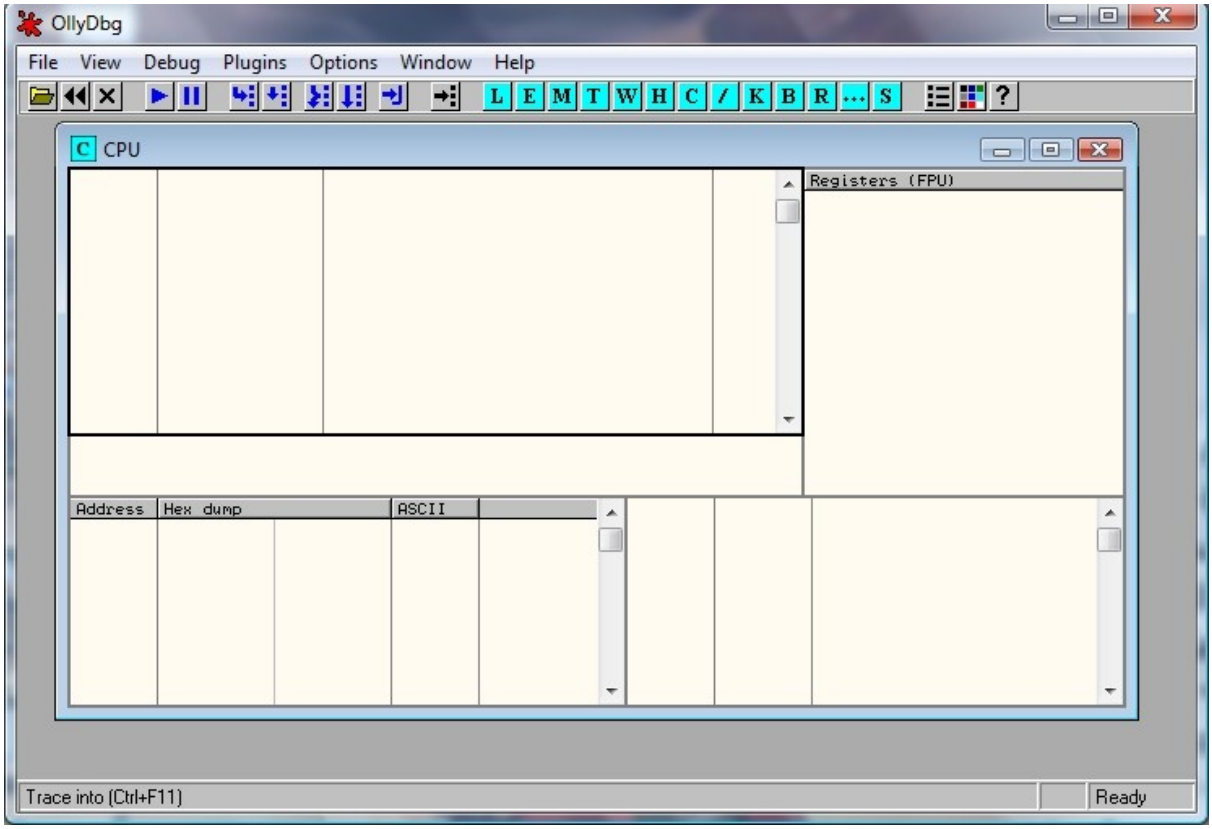
이제 울트라 에디트를 킵시다.



대사를 불러오면 요렇게 뜹니다. 동그라미(?) 쳐진 곳을 클릭해 16 진수를 보이게 합시다.

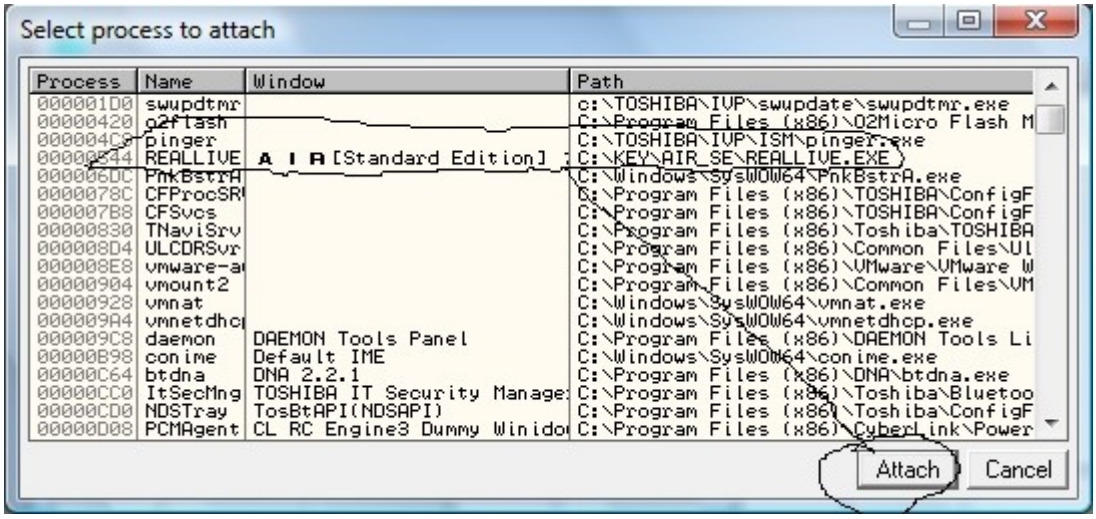


성공!! ^ ^
게임타이틀로 돌아갑니다.
이제 올리를 킵시다.

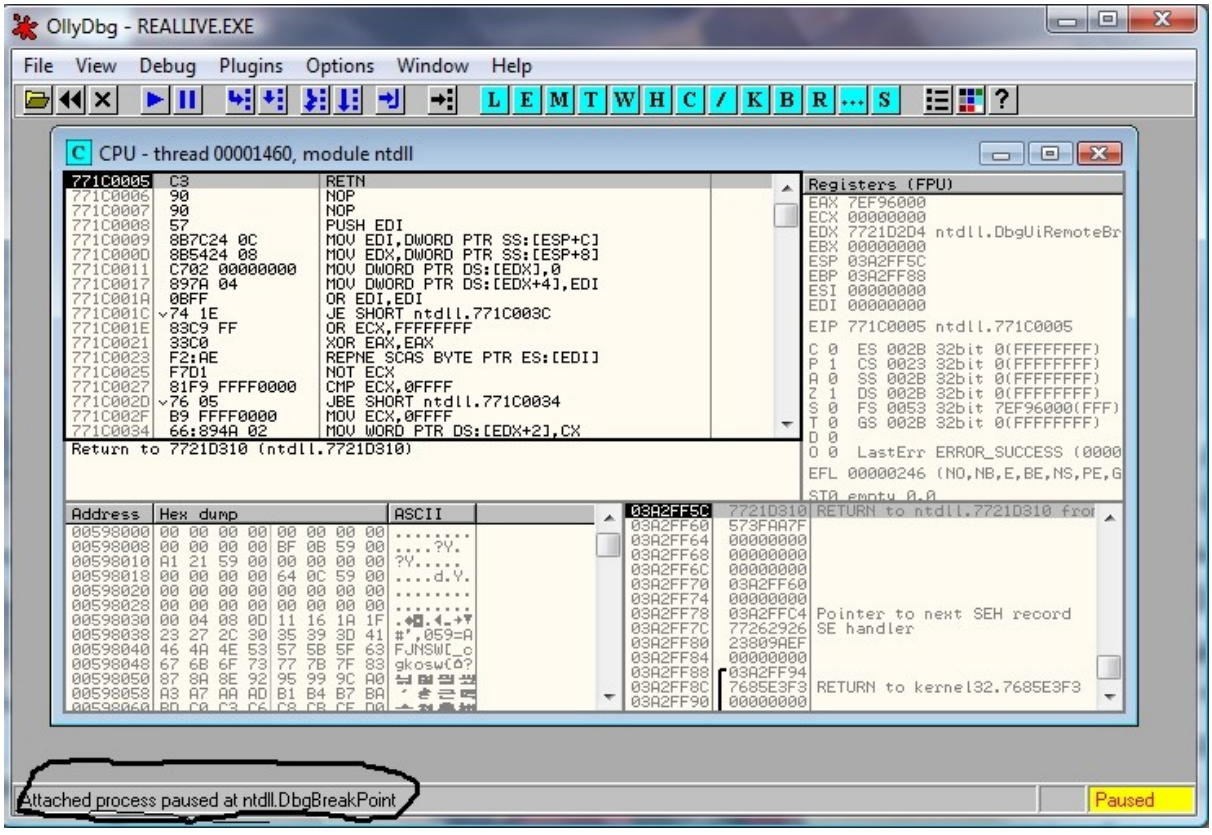


File 메뉴에 들어가 게임을 Attach 시킵시다.

이렇게.....

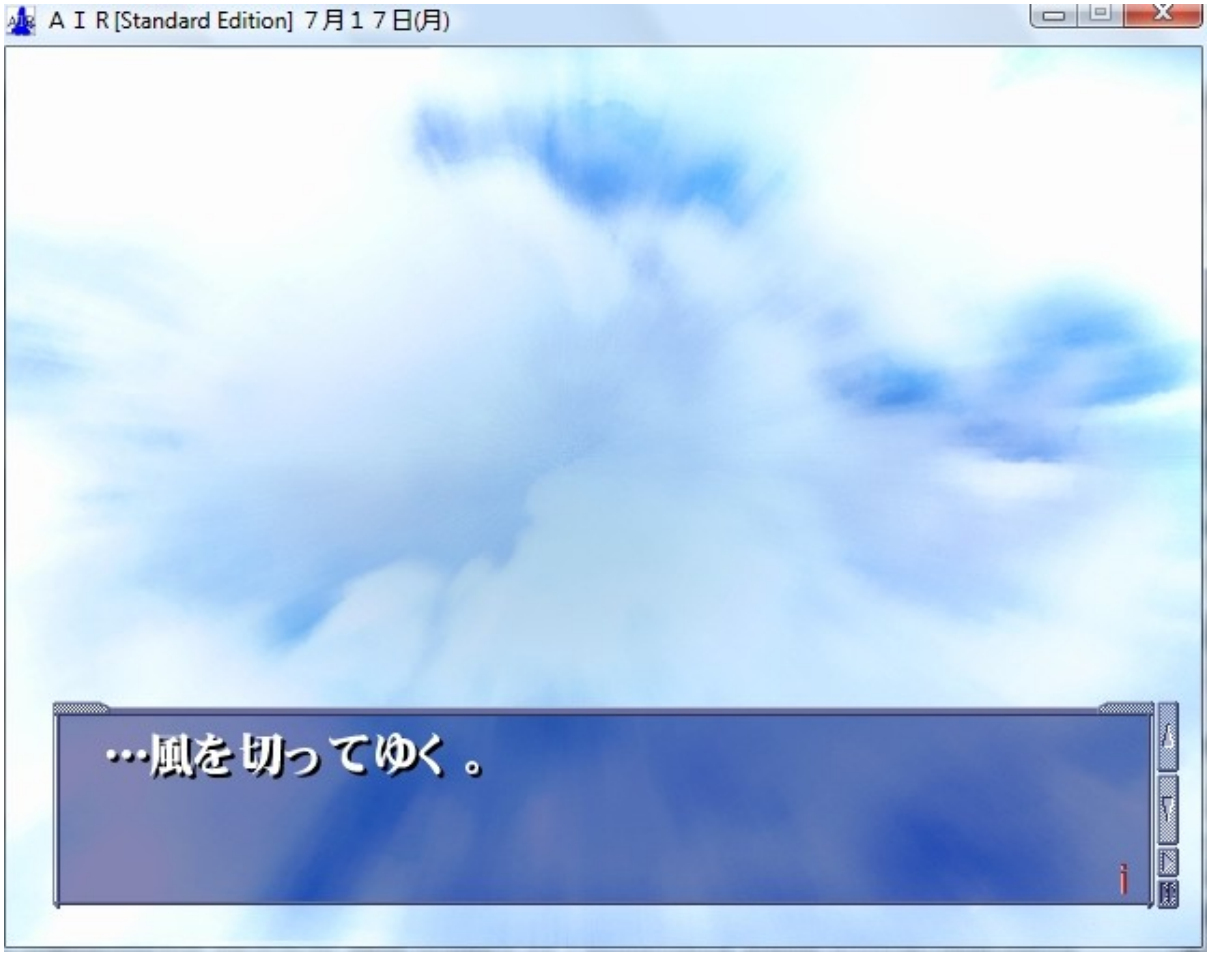


자 Attach 시킵시다.



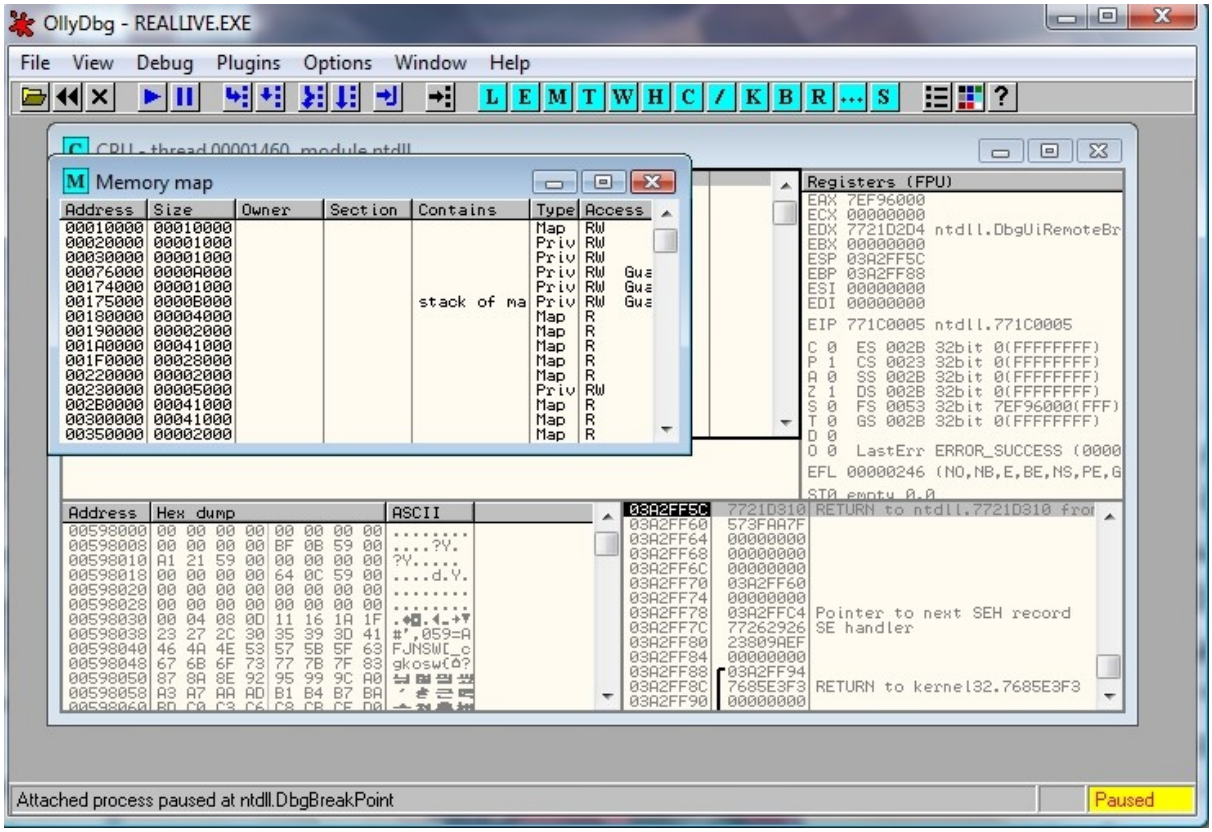
이 부분에서 멈출 겁니다. 살포시~~F9 을 눌러줍시다.

그 후, 게임을 수집한 대사 전!까지 진행합시다.

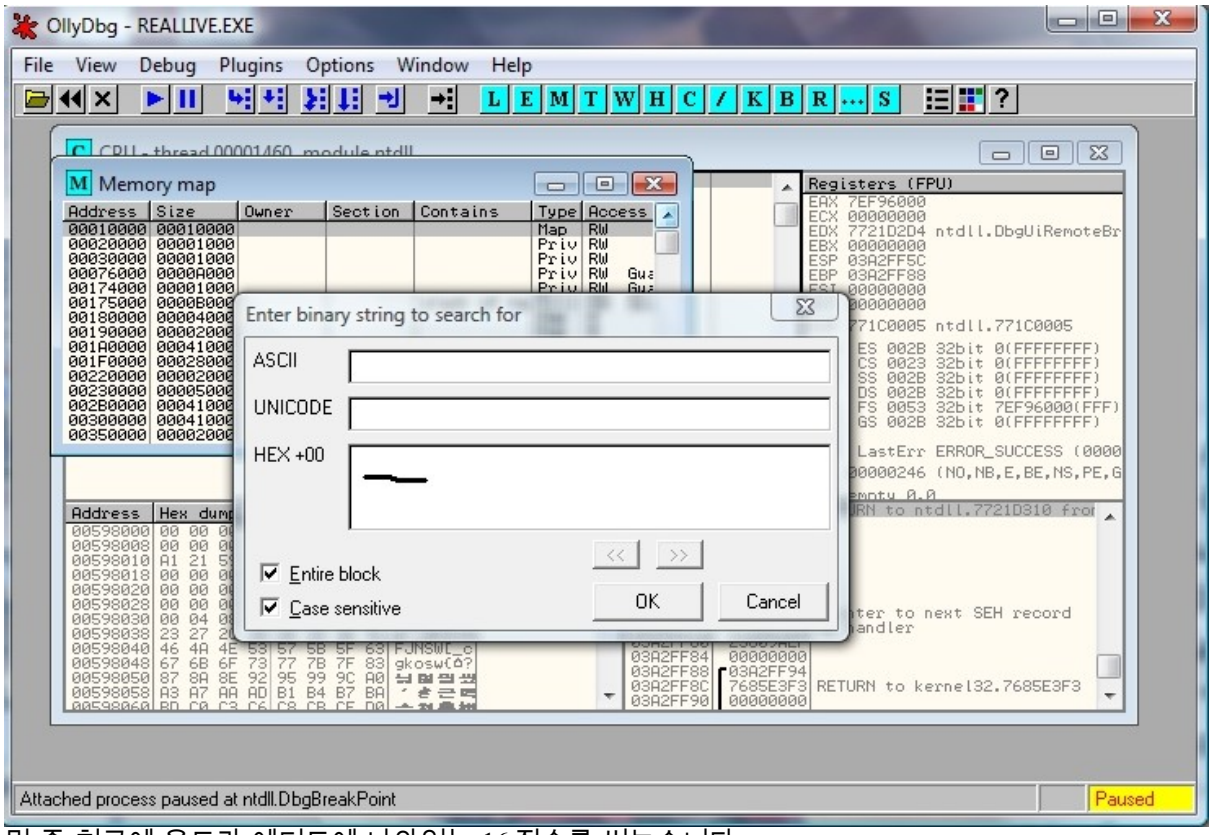


이제 본격적인 디버깅을 합시다.

위에 있는 올리 스샷에서 Alt+M 을 누르시면…

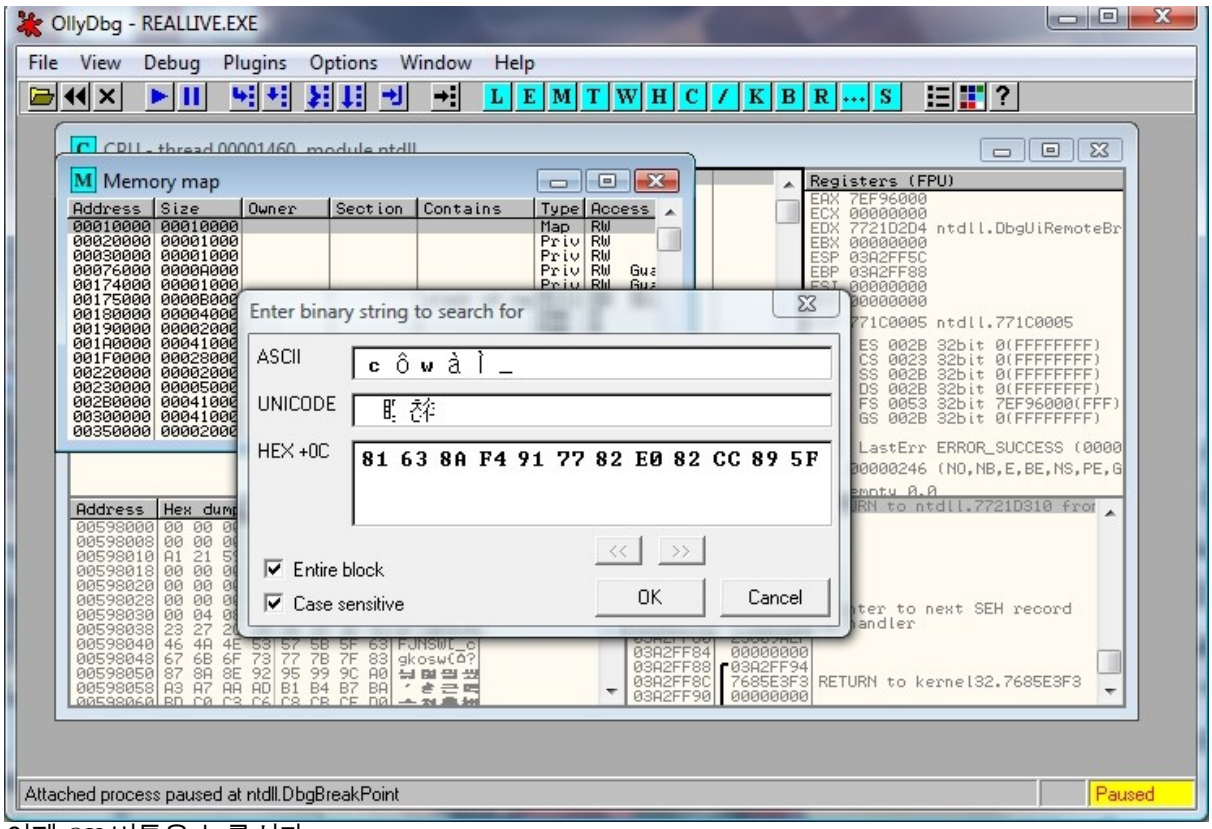


Memory Map 이 뜹니다. 그 후, CTRL+B 를 누르시면…

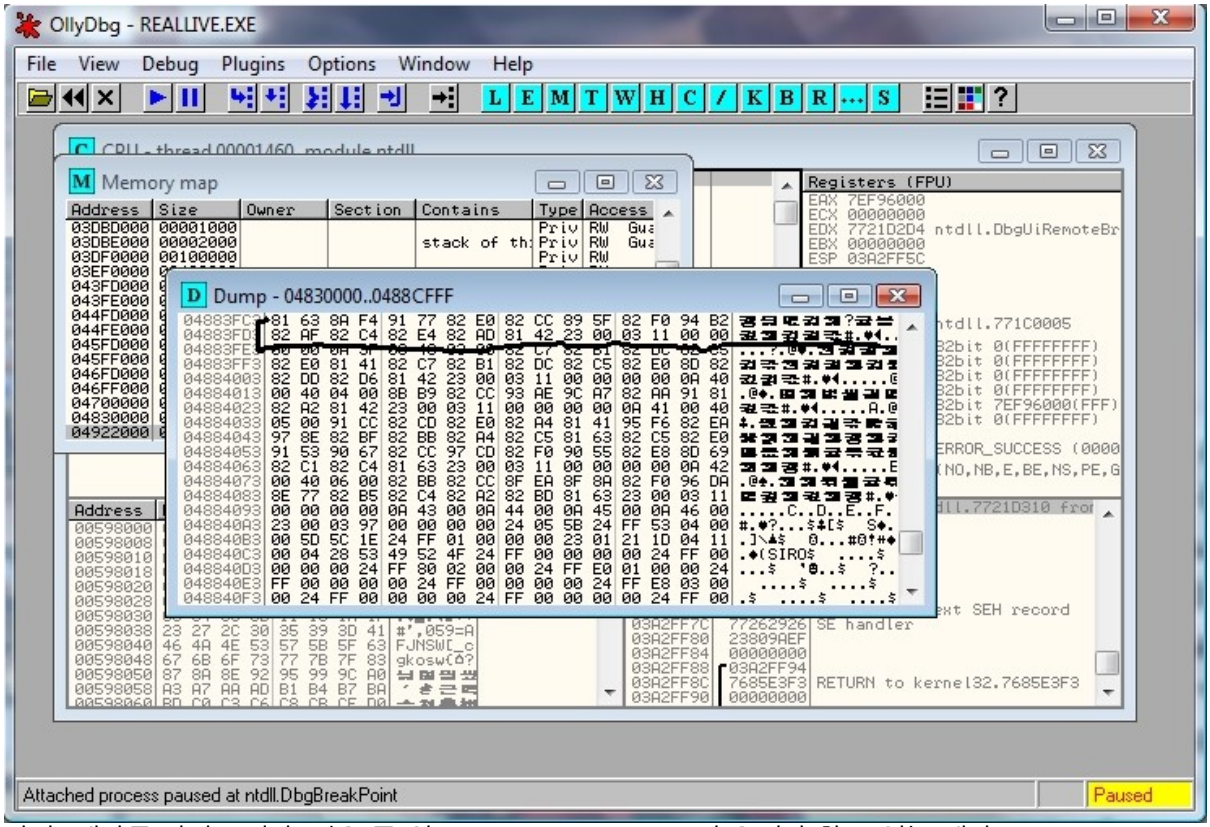


밑 줄 친곳에 울트라 에디트에 나와있는 16 진수를 써놓습니다.

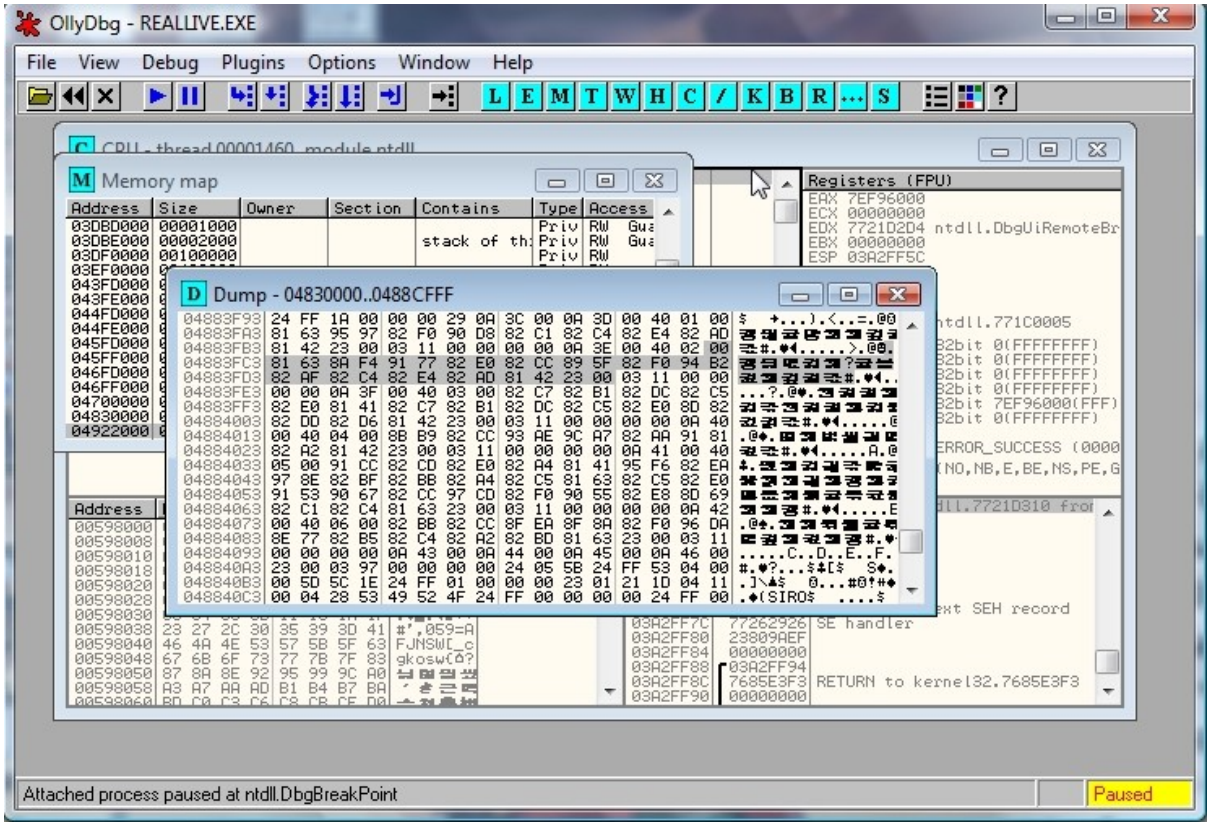
대사에 어느정도를 넣으면.....



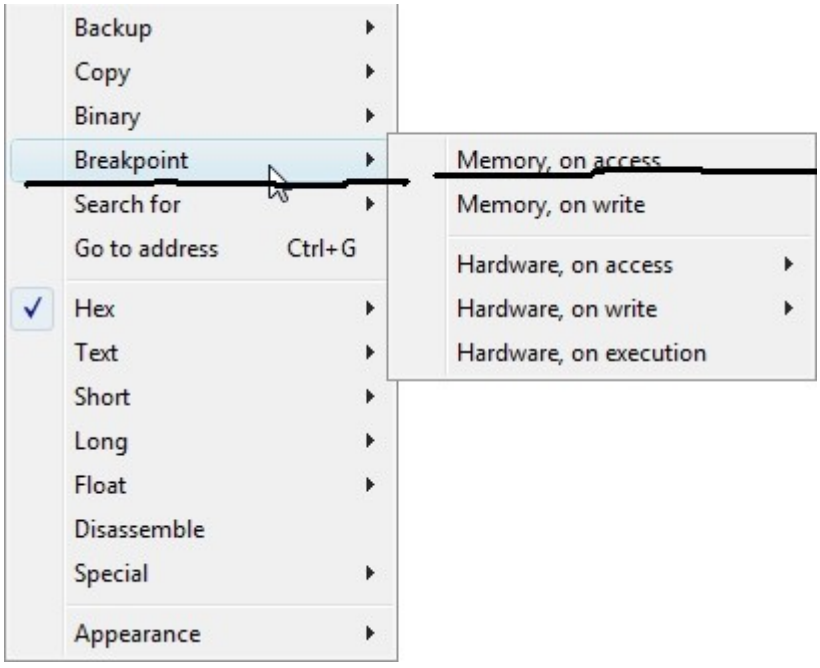
이제 OK 버튼을 누릅시다.



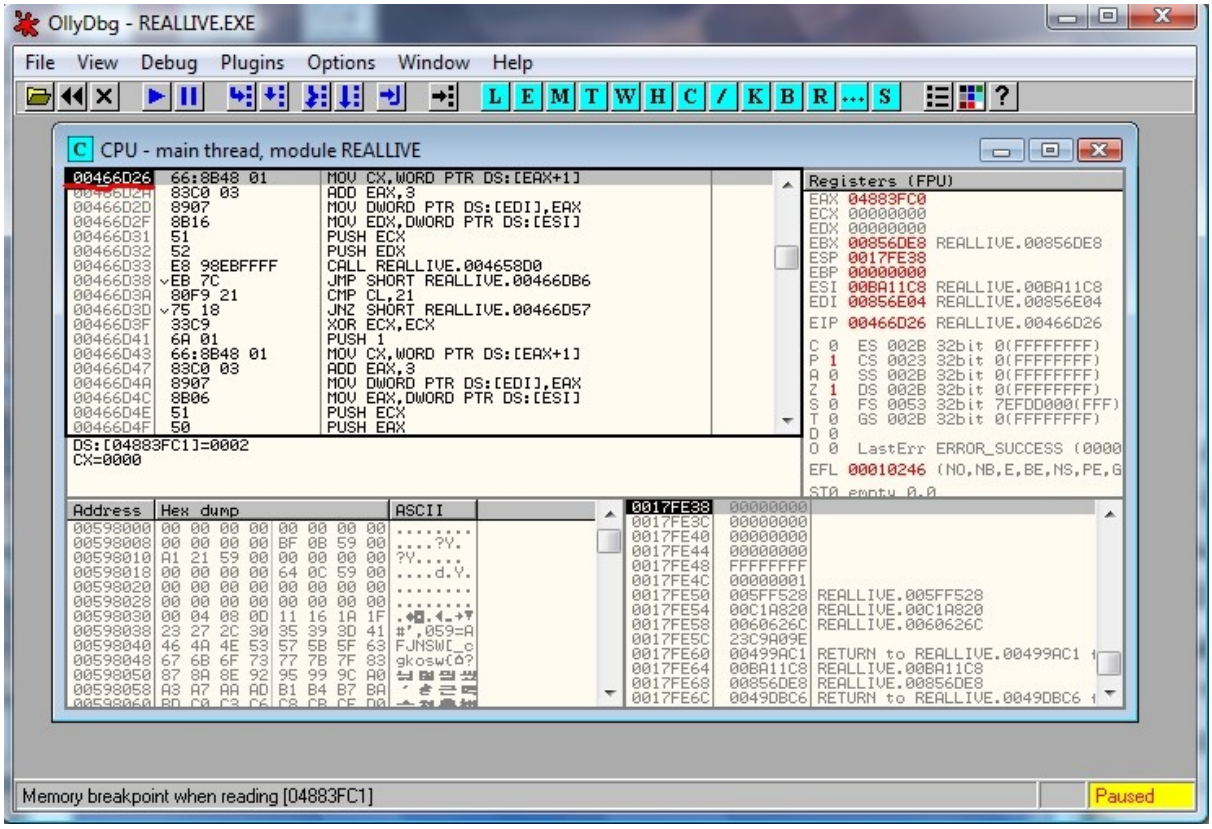
아자! 대사를 낚았습니다. 검은 줄 위로 81 63 8A…81 42 23 이 우리가 찾고 있는 대사.



대사 앞에 있는 00 부터 끝에 00 까지 선택 후, 마우스 오른쪽 버튼을 누릅시다.



브레이크 포인트를 이렇게 걸어줍시다.



저기 위에 빨간색으로 밑줄 쳐진게 대사 코드. 옆에 보면 MOV 어쩌구 저쩌구 밑으로 Add Eax 3. 더 밑으로 MOV 어쩌구 저쩌구.

즉, 최종코드는 466D26 EAX+3.

이제 선택지를 공략해봅시다.

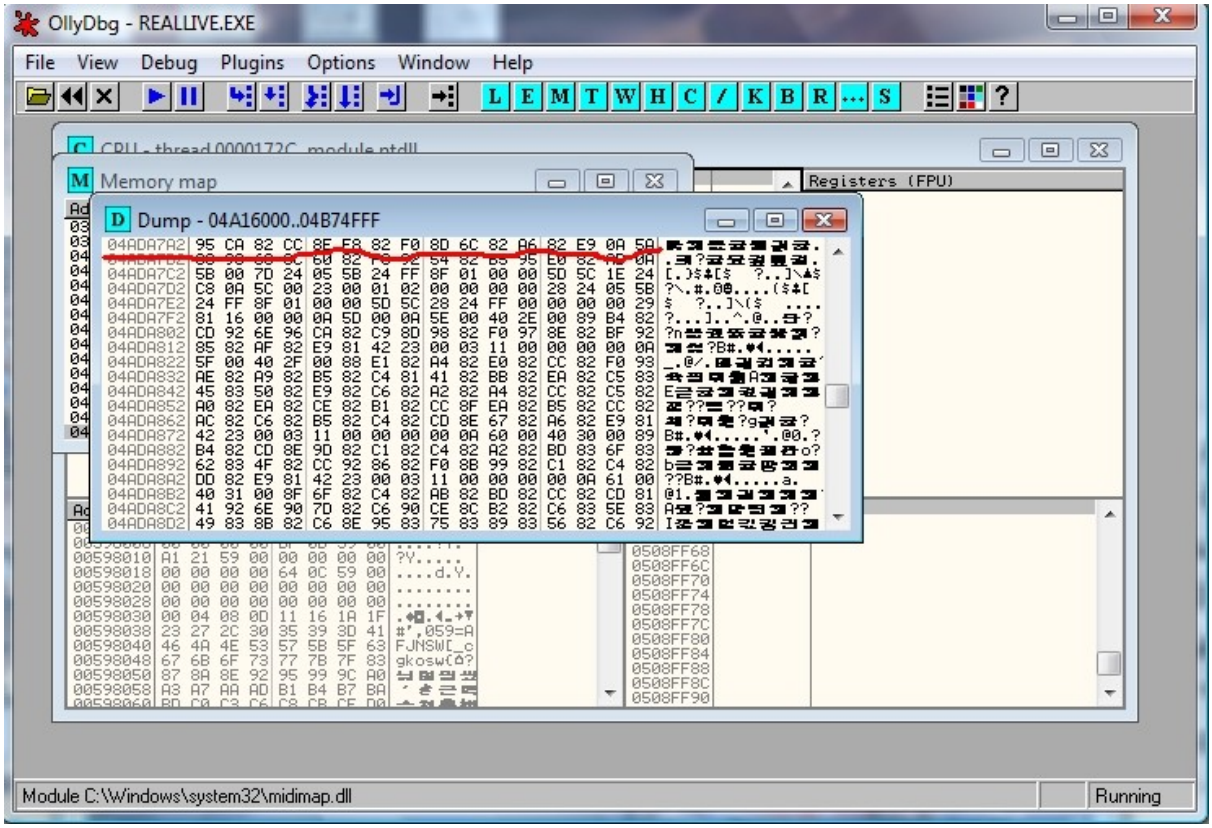
선택지를 대사와 같이 울트라 에디트로 불러와 16 진수를 표기해 줍시다.

일단 게임을 끄시고 (올리를 종료해서) 다시 시작하시는 것을 추천합니다.

자, 이제 게임을 키시고, 올리를 먹이고, 게임을 선택지 전! 까지 진행해 줍시다.

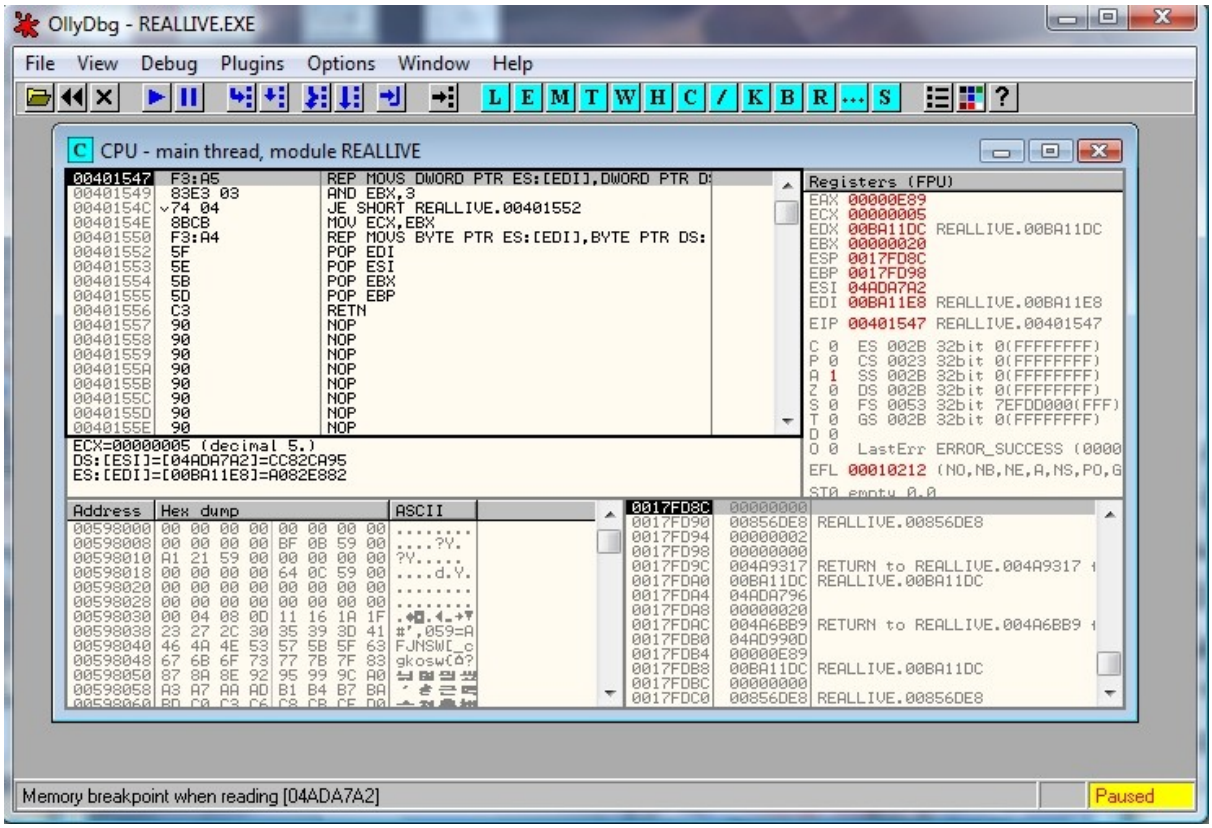
AIR 에선 이렇습니다.

대사와 같이 올리에서 선택지 문장을 낚습니다.

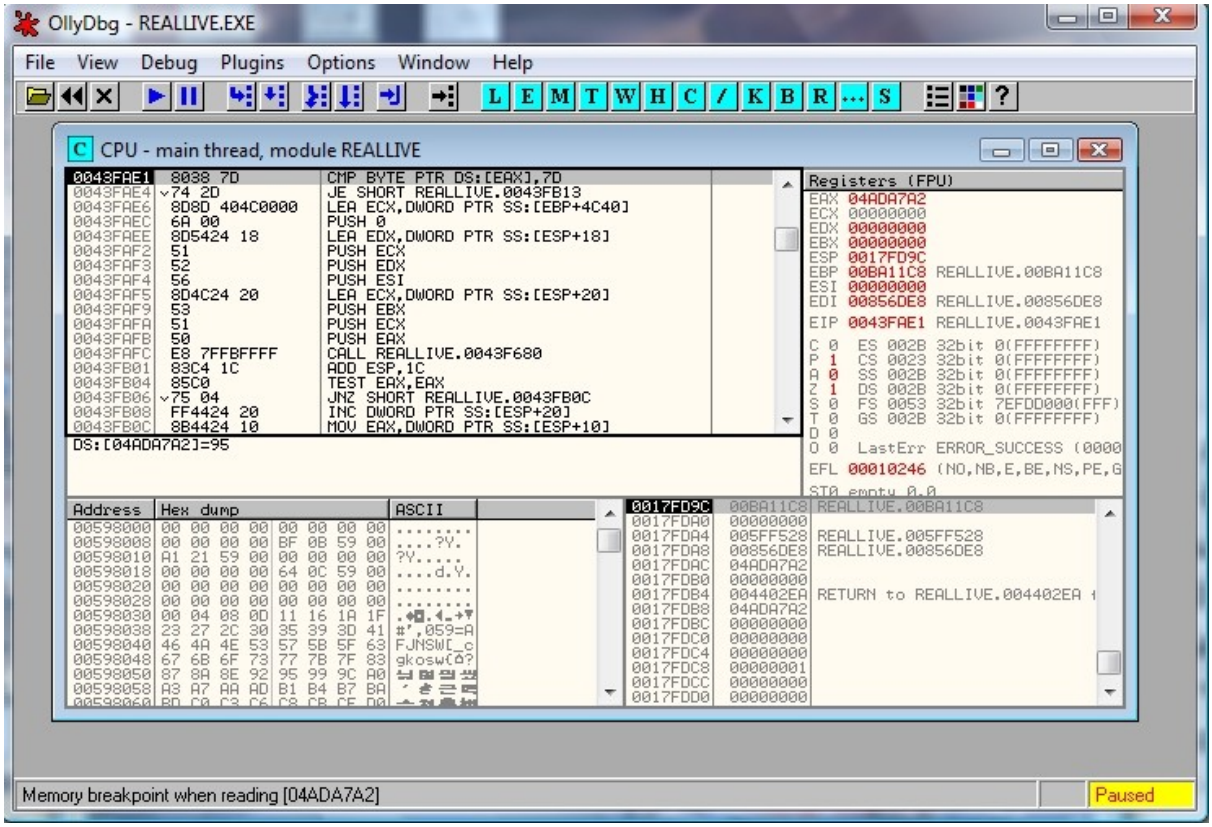


밑 줄쳐진게 선택지 문장. 대사는 00 으로 시작해 00 까지 선택해 주었지만, 선택지 문장은 00 아닌 숫자로 시작해 00 아닌 숫자로 끝냅니다.

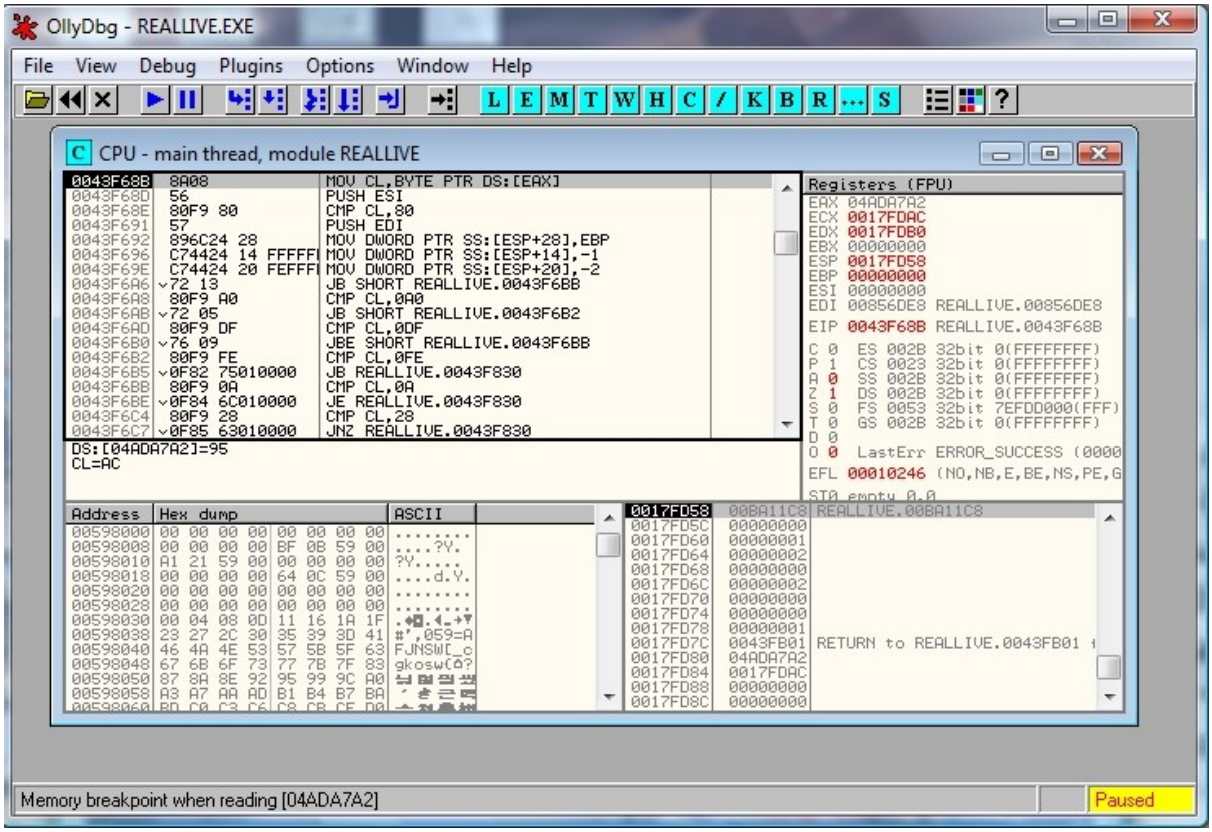
그 후, 브레이크 포인트를 걸면.....



보면 REP 어쩌구 저쩌구 합니다. 요놈은 아니니...
F8 을 누른후 F9 을 누릅니다.

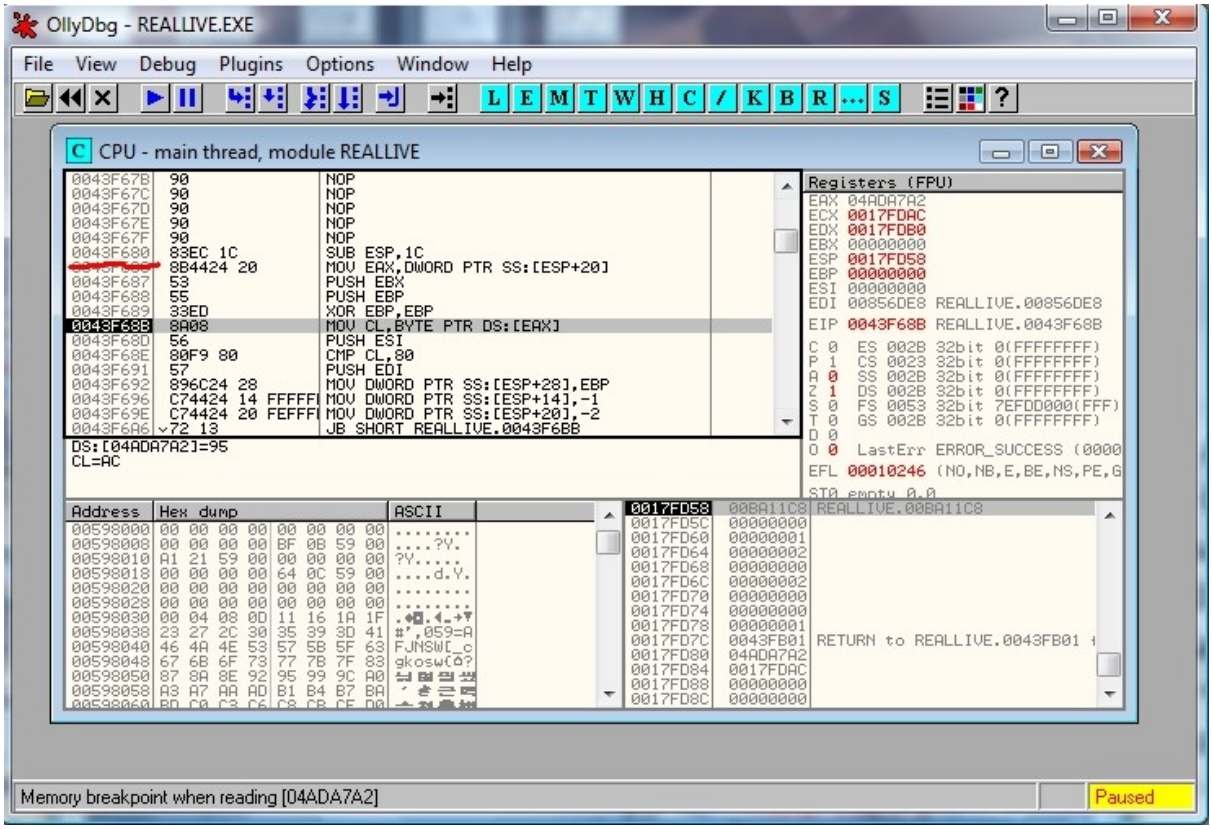


CMP 어쩌구 저쩌구..요놈도 아냐....
F8 을 누른후 F9 을 누릅니다.



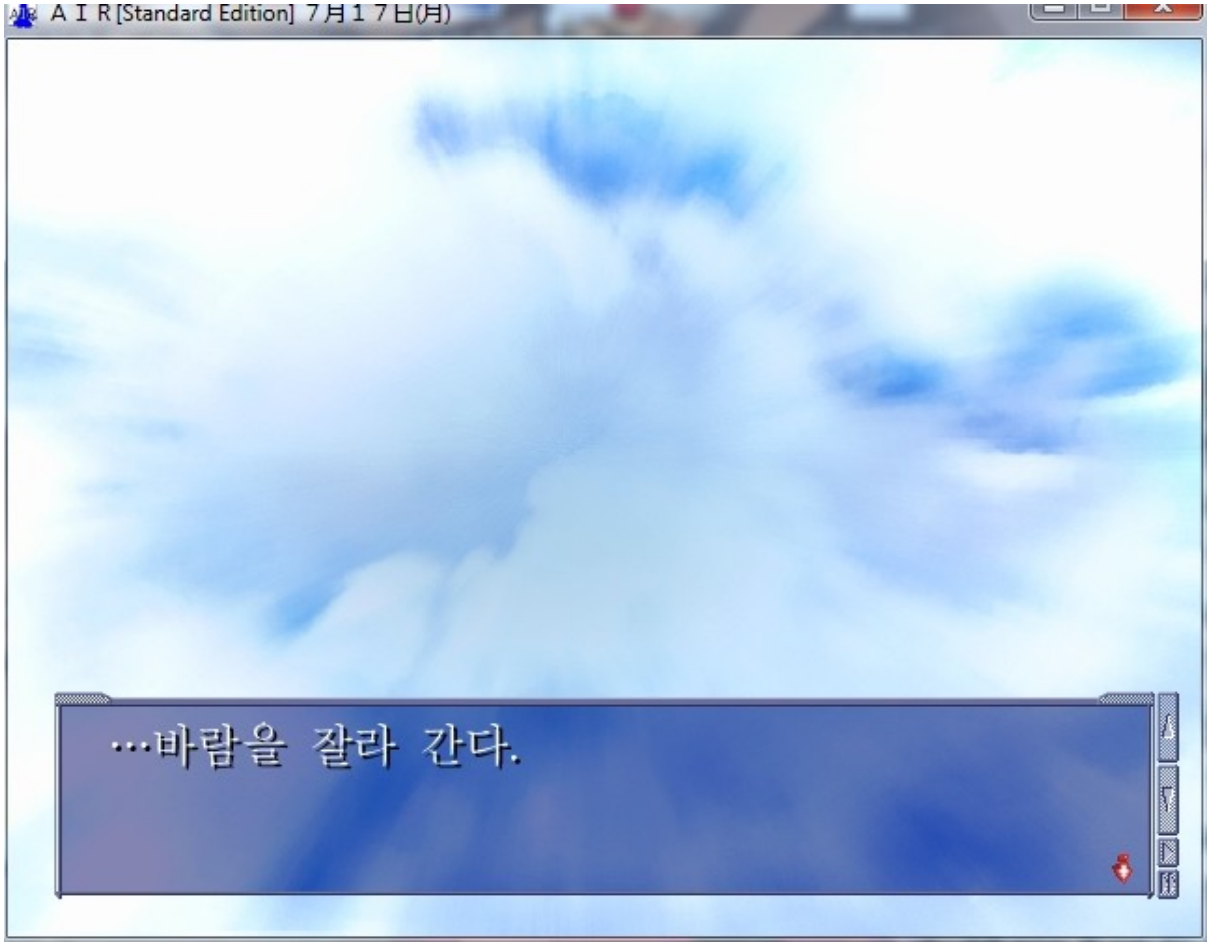
찾았다.
이제 스크롤 업을 합니다. 조금만.

그럼...



밑 줄쳐진 곳이 코드. 43F680 ESP+4. ESP+4 는 옆에 SUB ESP, 1C 그리고 밑으로 어쩌구 저쩌구 하는 것을 계산해야합니다. 전 못하므로 패스!!! 거의 대부분 ESP+4 을 쓰면 맞습니다.

이제 게임에 코드를 먹이면.....(스크립트 덮어쓰기와 RLcmd 필터, 한글폰트 불러오는 것 잊지말아주세요 ^ ^)



성공!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

끝입니다. 간단합니다.