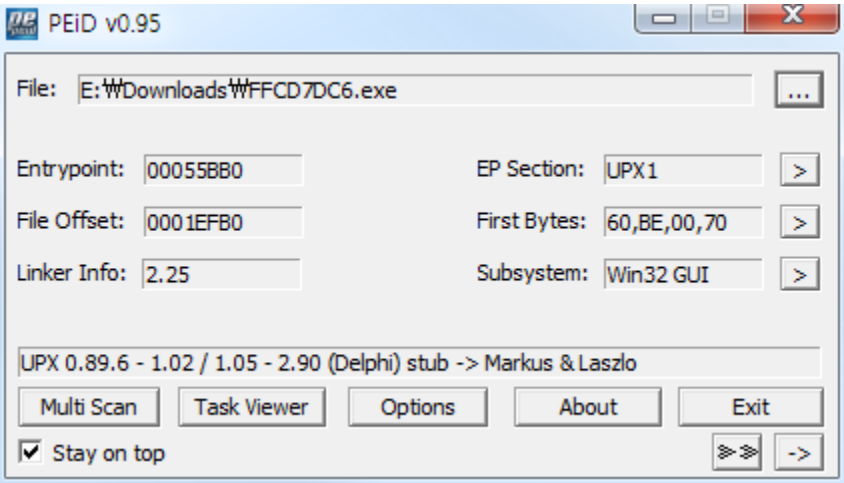
4번 문제 갖고 한 시간 정도 헤맸는데 알고 봤더니…… unpack 문제였다.



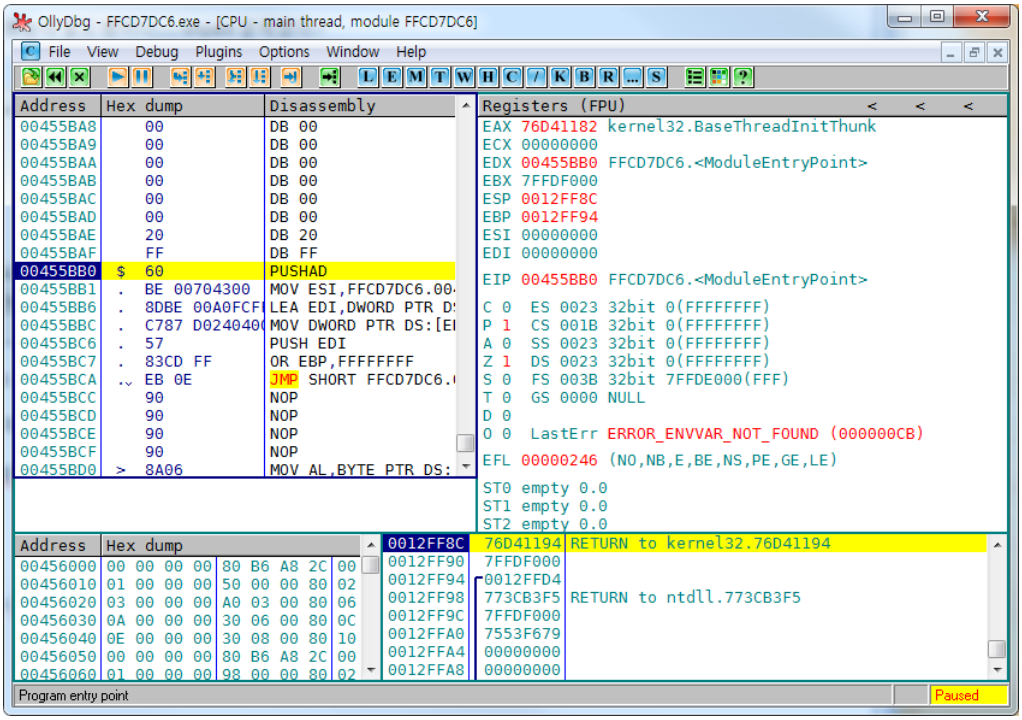
사진을 보면 EP Section에 UPX1과 아래 UPX 0.89.6 이라는 문구가 있는 것을 알 수 있다.

예전 기억을 더듬어 보면 패킹이 되어 있으면 항상 ㅎㄷㄷ 했었는데… 지금도 역시 그렇다.

하지만 한번 해보니 UPX1은 블로깅이 많이 되어 있어서 쉽더라.

아무튼 한번 해보겠다.

일단 UPX는 시작 시에 PUSHA로 모든 레지스터 내용을 스택에 보존 시킨다.



위 사진이 그것인데 PUSHA로 되어 있는 것을 알 수 있다. 그리고 OEP로 점프하기 전에 POPAD로 레지스터 내용을 복구한다.

여기서 OEP가 무엇이냐 면 Orignal Entry Point의 약자입니다. Entry Point란 프로그램이 최초로 수행되는 코드 즉, 진입점 함수를 말합니다.

C에서 보면 main함수가 되겠네요. (사실 main함수가 아니죠?? Windows에서는 xxmainCRTStartup, 리눅스에서는 __libc_start_main이 main함수를 실행시킵니다._)

아무튼 우리는 OEP를 찾아야 합니다. 왜냐하면 패킹이 되면 EntryPoint가 우리가 원하는 프로그램 시작지점이 아니게 되기 때문입니다.

우리가 원하는 건 main함수 같은 그런 시작지점입니다.

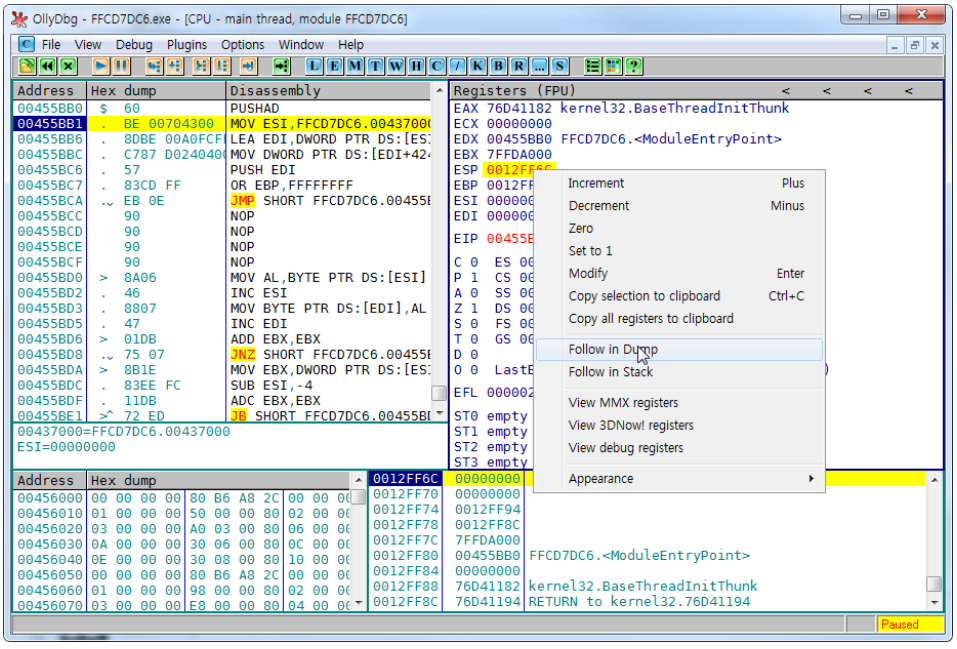
블로깅된 정보를 보니 ESP를 이용해서 하드웨어 포인터를 사용해서 하더군요.

잠깐 unpacking 순서를 쫙 펼쳐보자면…….

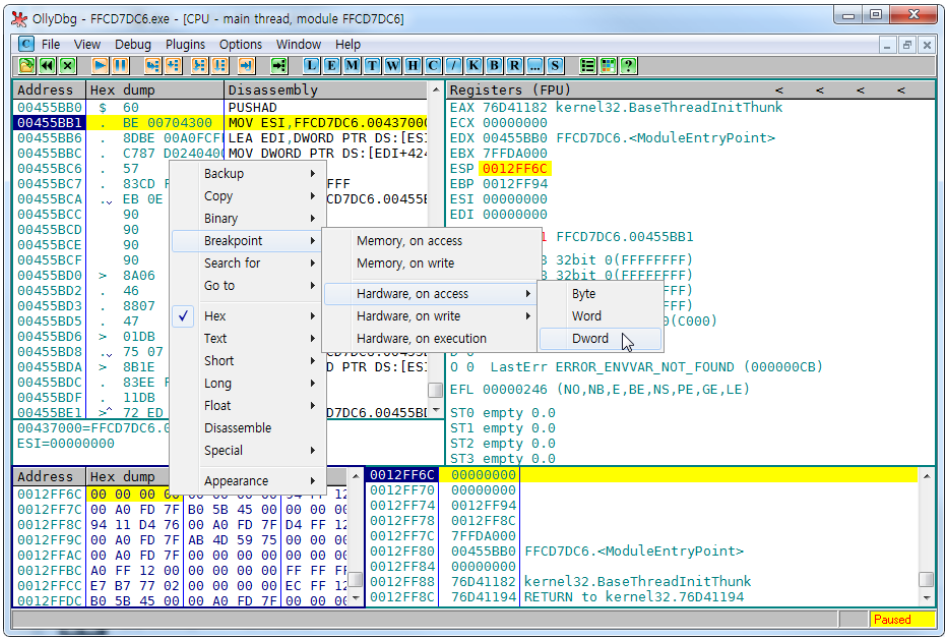
ESP에 하드웨어 브레이크 포인트->실행->Olly Dump->Rebuild Import 해제 후 빌드->OEP 저장->패킹된 프로그램 시작->Import REC시작->Attach Process->OEP 입력->AutoSearch->Get Imports->Fix Dump 이 순서로 이루어 지더군요.

하나씩 따라가면서 해보도록 하겠습니다.

먼저 원하는 프로그램을 OllyDebuger(이하 올디)로 엽니다.

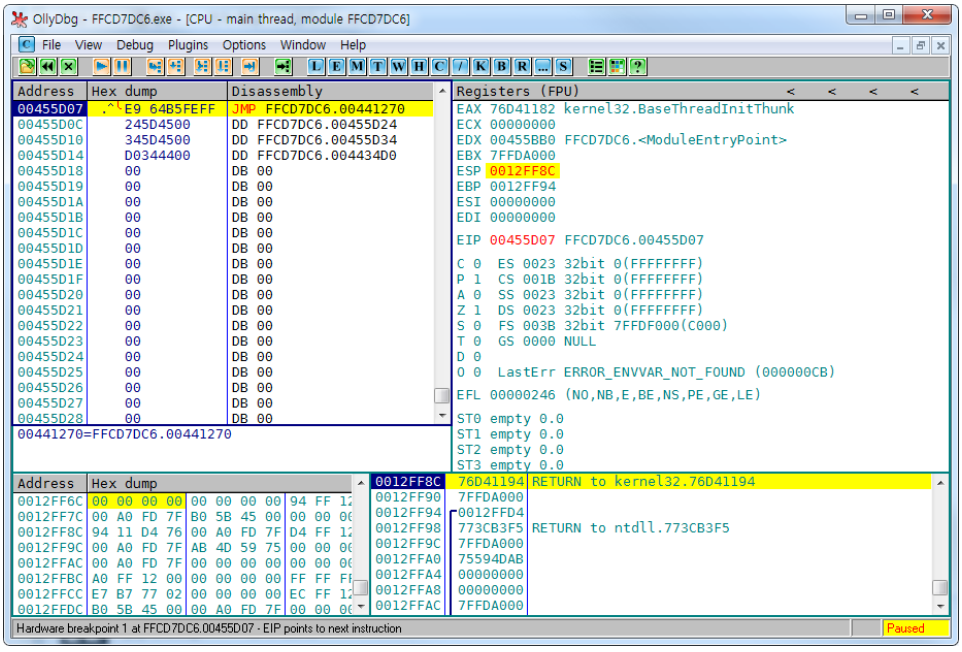


위 그림과 같이 한번 실행한 후 (step over) Folliow In Dump를 해서 아래 메모리 창에 데이터가 나오게 합니다.



그리고 4바이트를 선택한 후 Hardware Break Point를 겁니다. DWORD로요. 왜냐하면 처음 시작 부분에 보시면 알겠지만 PUSHAD라는 명령어가 있죠? 마지막에는 POPAD라는 명령어가 있습니다. 그 후 OEP로 점프하게 되는데 우리는 그 지점을 찾고 싶은 겁니다.

아무튼 하드웨어 브레이크 포인트를 설정하셨으면 F9를 눌러서 실행해 주세요.

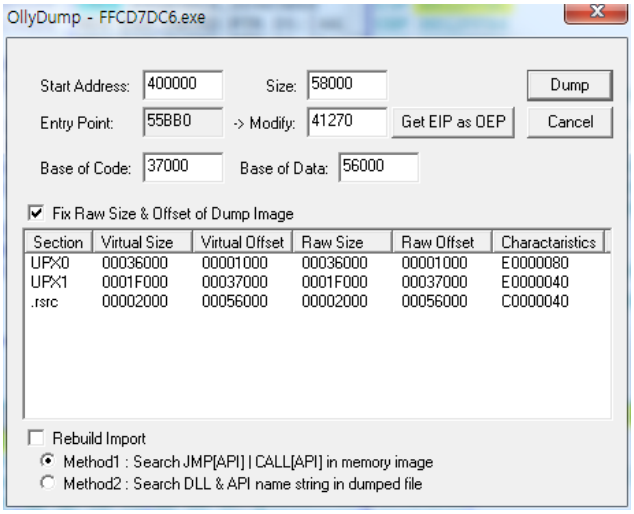


그럼 위 그림과 같이 점프 구문으로 이동하게 됩니다. 그 곳이 바로 우리가 원하는 OEP로 점프하는 구문입니다.

자 F8을 눌러 봅시다. 어?? 왔네요… PUSH EBP로 시작합니까? 그럼 OEP를 맞게 찾으신 겁니다. 이제 다 성공하셨네요.

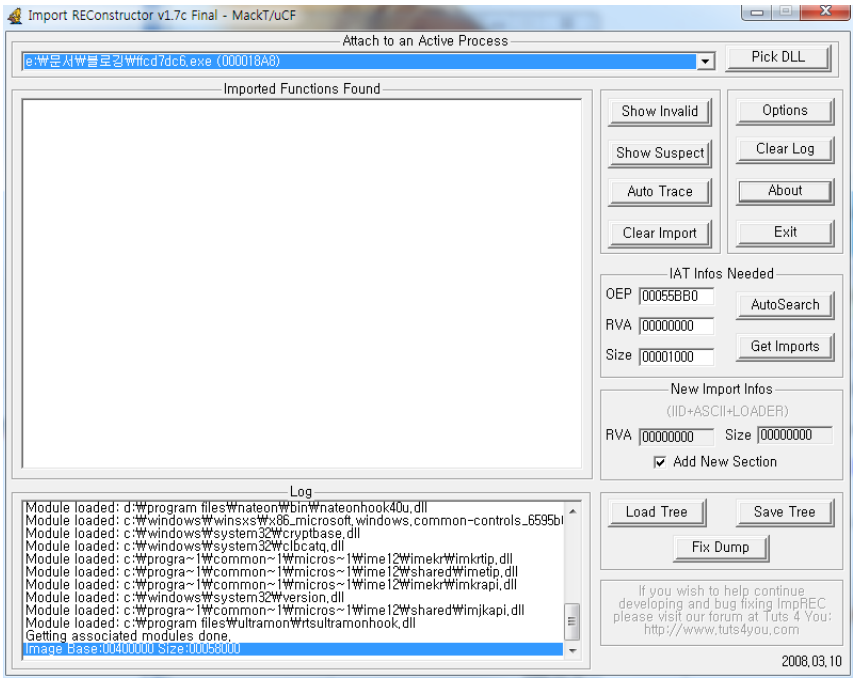
이제 Plugins를 눌러서 OllyDump를 실행해 주세요. 없으시면 다운 받으시면 됩니다. 구글에서 검색하니 바로 나오더군요.

이 플러그인의 역할은 현재 메모리를 덤프 뜨는 거라고 합니다. 우리는 현재 엔트리 포인트에 있기 때문에 이 쪽을 덤프뜨게 됩니다.

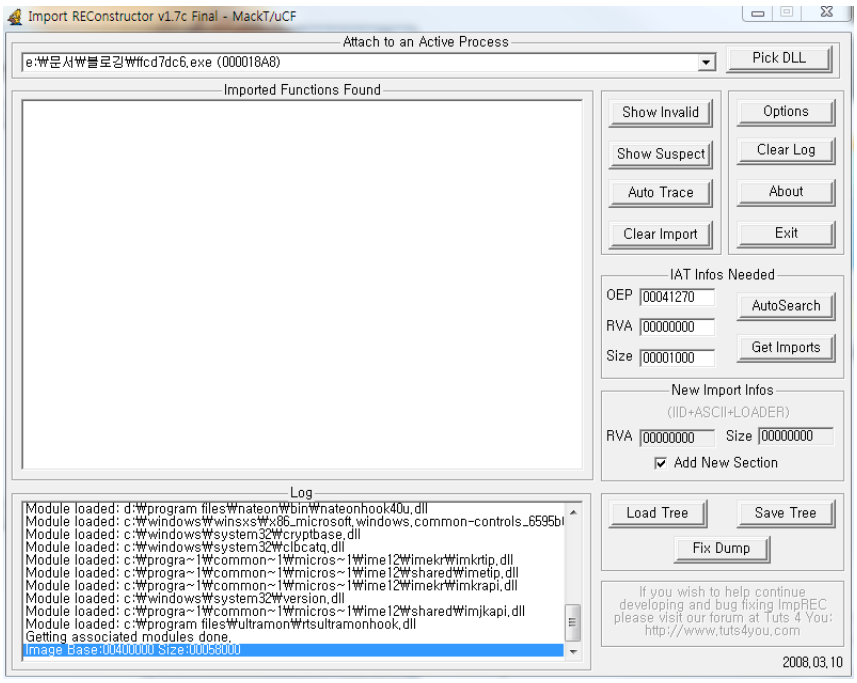


주의 하실 점은 Rebuild Import를 해제해 주세요. 올디가 IAT를 재구성해 주는데 잘 안 된다고 하네요. 그 후 Dump를 해주시면 됩니다. 파일이름은 대충 맘에 드시는 걸로 지우시되 Entry Point를 저장해 주세요. 저는 41270 이네요.

그 후 Import REC라는 프로그램을 다운 받아서 실행시켜 주세요. 그리고 언패킹할 프로그램도 실행시키시구요.



Import REC는 IAT를 복구 시켜주는 툴인데요. OEP가 필요합니다. 하지만 우리가 아까 OEP를 찾았죠?? 그걸 입력해 주시면 됩니다. 자 해볼게요.



OEP에 Entry Point를 입력했습니다. 그 후 AutoSearch, Get Imports를 누르시고 Fix Dump를 누르세요. 파일 저장은 아까 올디에서 메모리 덤프했던 그 파일을 선택해주시면 됩니다. 그러면 성공했다는 메시지와 함께 IAT가 복구됩니다.

실행하면 잘 실행되네요.