

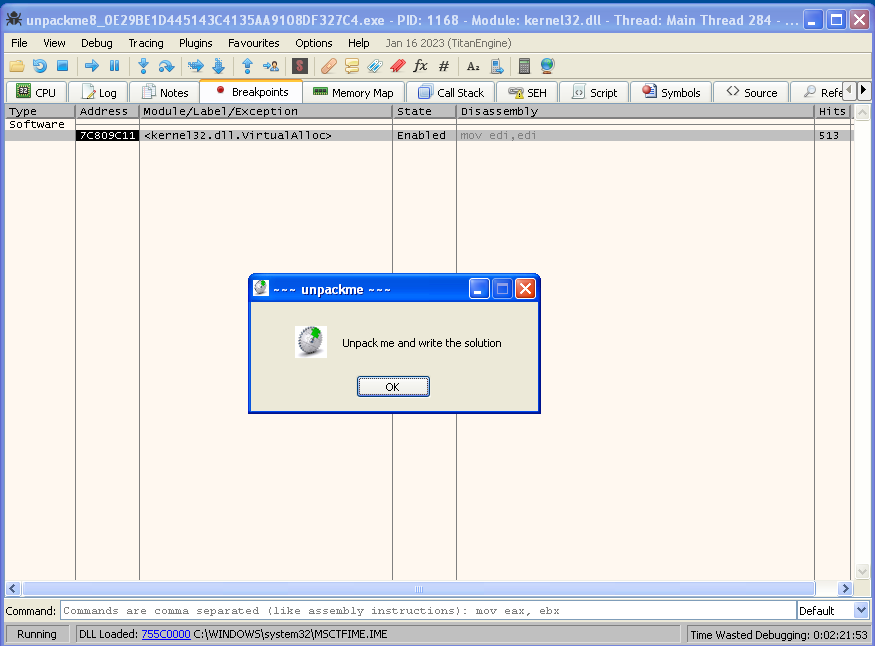
Sử dụng LoadLibraryA() và GetProcAddress() xác định được con trỏ hàm của

* RtlAllocateHeap
* RtlFreeHeap
* VirtualAlloc

Sử dụng LoadLibraryA() và GetProcAddress() để khôi phục IAT

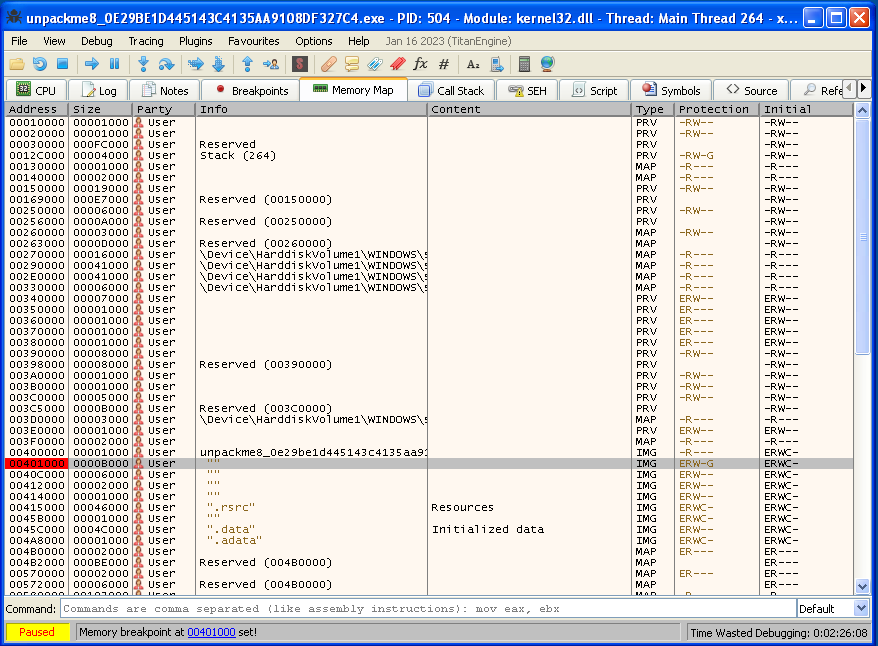
BP VirtualAlloc

Sau đó F9 đến hit thứ 514 thì chương trình chạy hoàn toàn

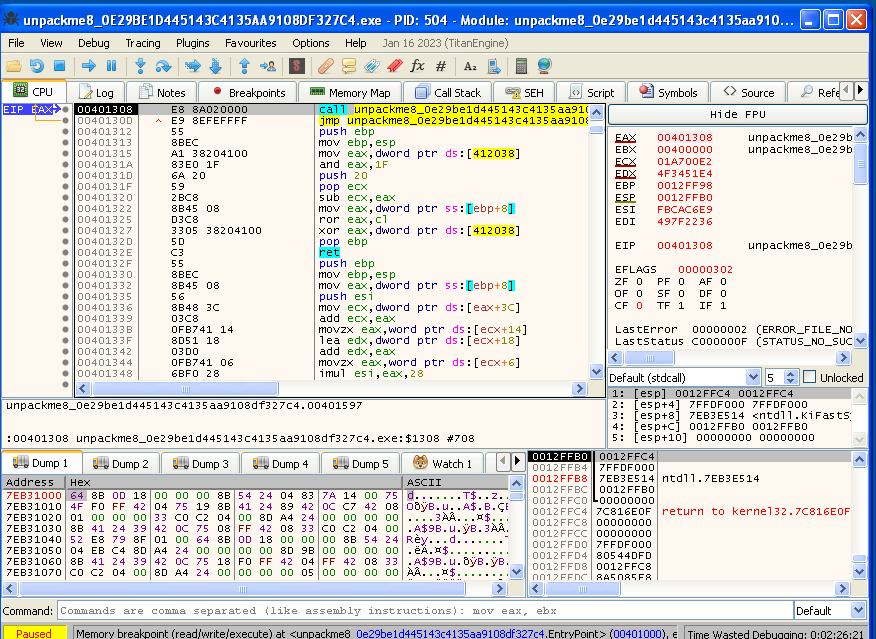


Tiếp tục làm lại như trên nhưng chỉ chỉ chạy 513 lần

Sau đó set memory breakpoint access vào section .text và F9



F9 để chương trình nhảy vào section text



Dùng scylla để dump file