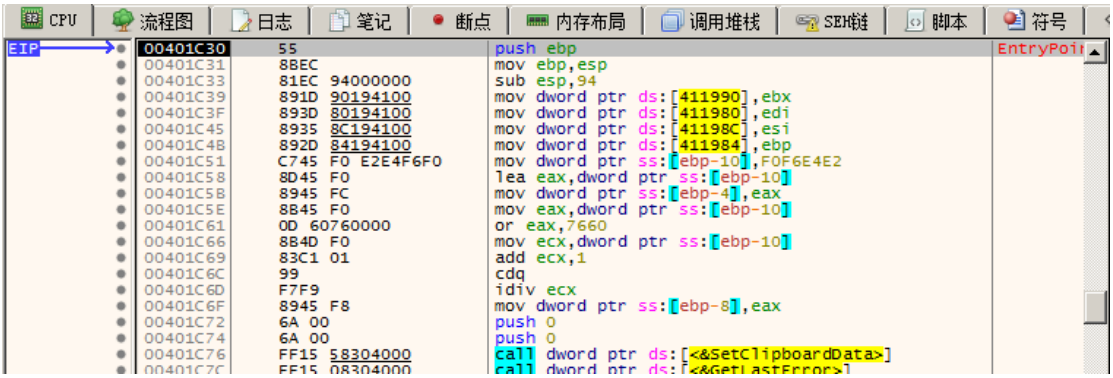
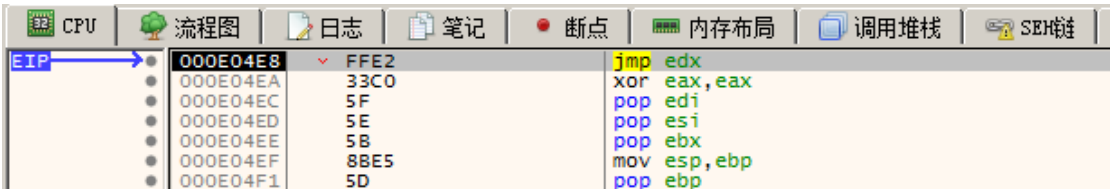
>> 抓病毒行为：重点是 exchange1.dll 这个释放文件；
oledump.py 尝试获取一下 office 文件中的宏代码；
https://blog.csdn.net/Cody_Ren/article/details/79941643

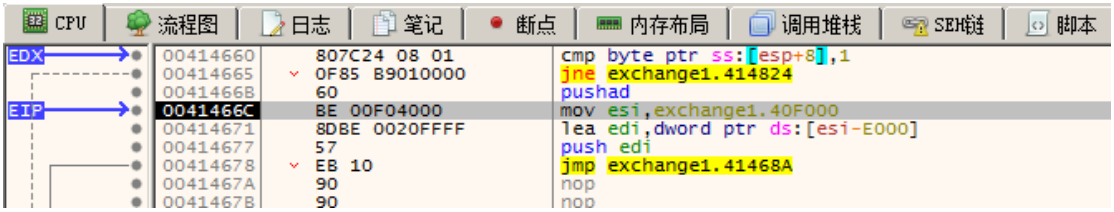
>> 对其脱壳：
push ebp 之后 esp 定律



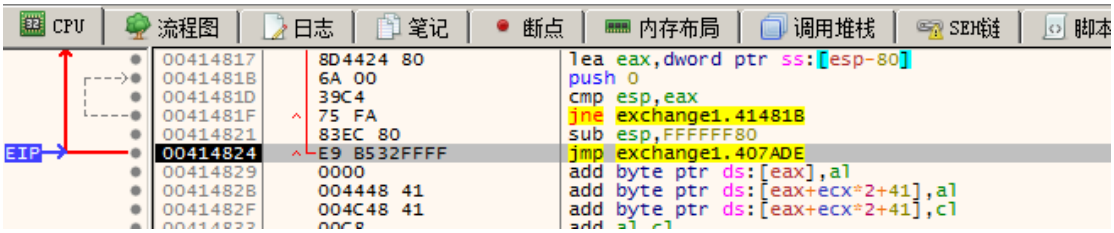
go 一下：



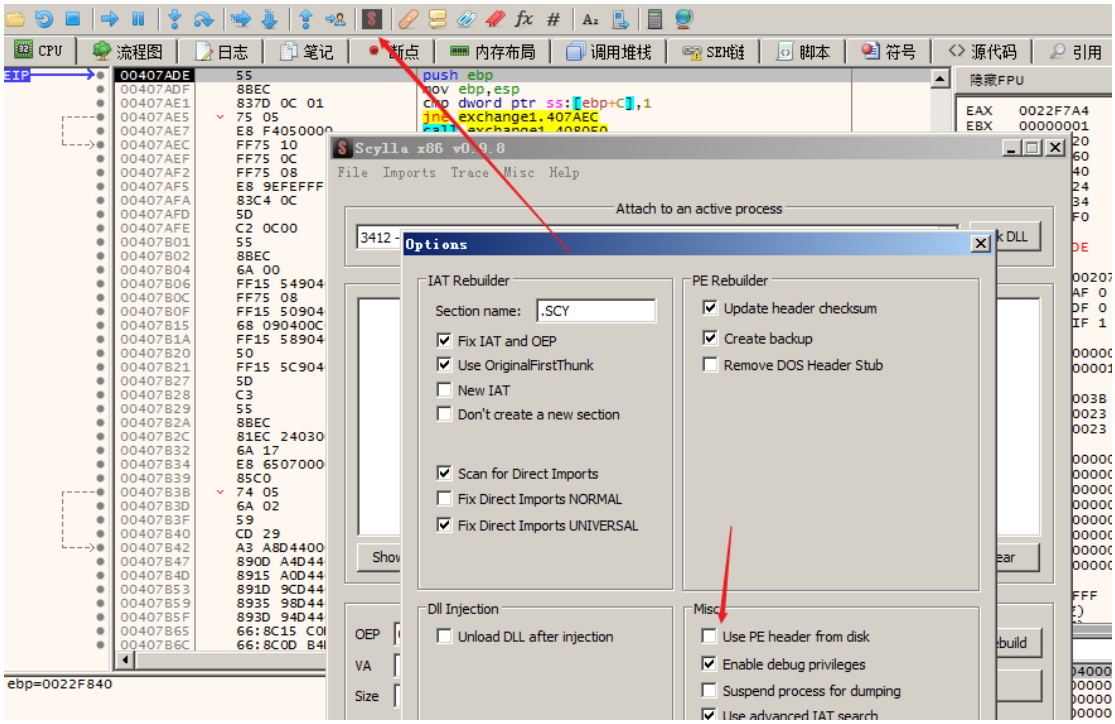
pushad 后再次 esp 定律



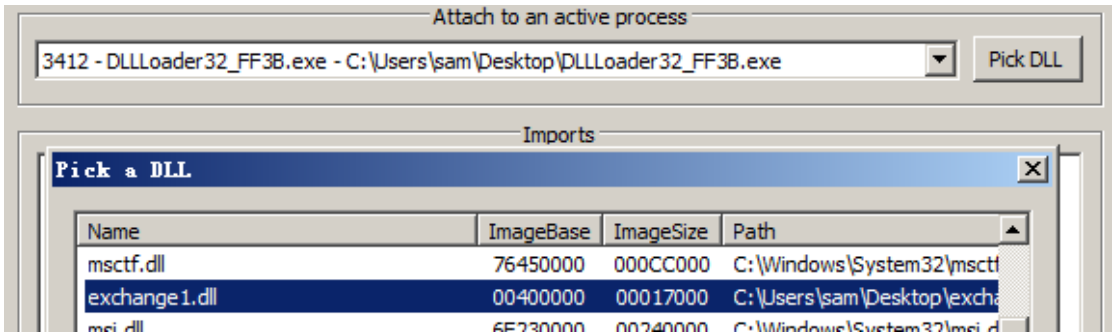
go

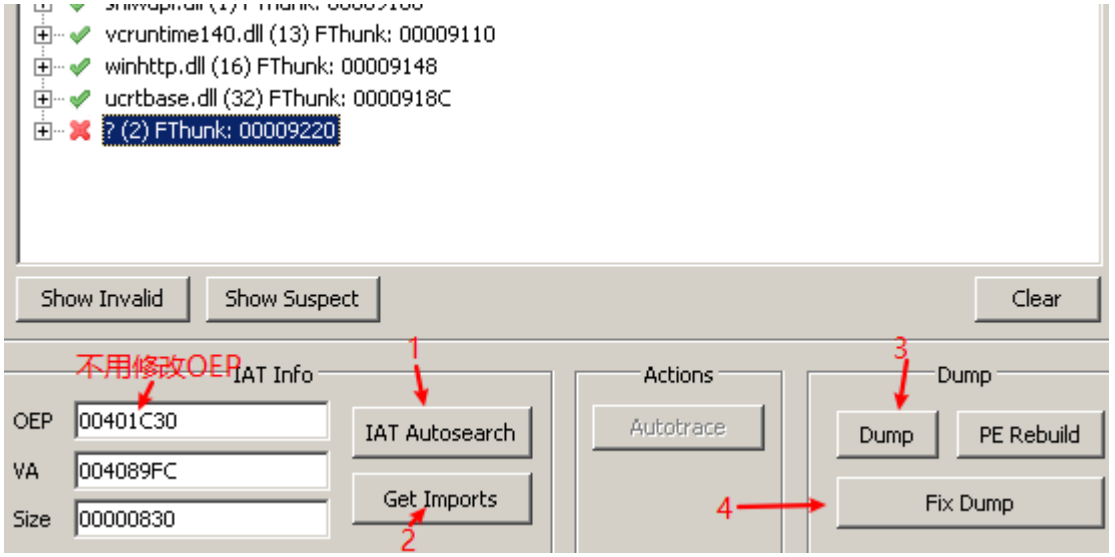


jmp 跳过去，开始 dUmp，先设置一下：

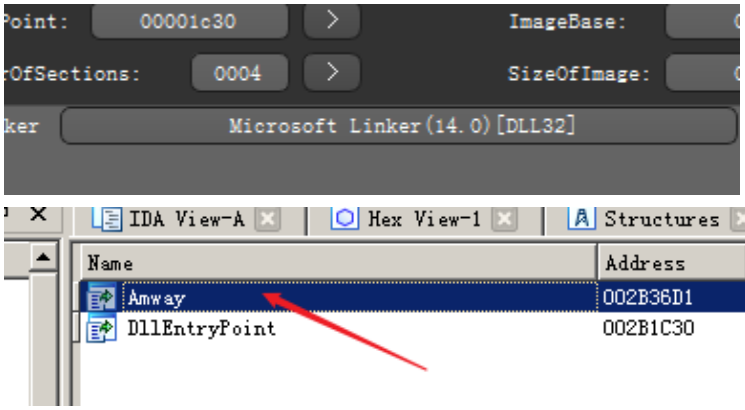


pickDLL 选择





脱壳完毕，静态分析即可。



>> 也可以带壳调试：
根据 bp VirtualAlloc 下断，不断 F9 反汇编观察返回到。来自的地址，查看参数地址内容即可。

https://www.pianshen.com/article/32721181205/