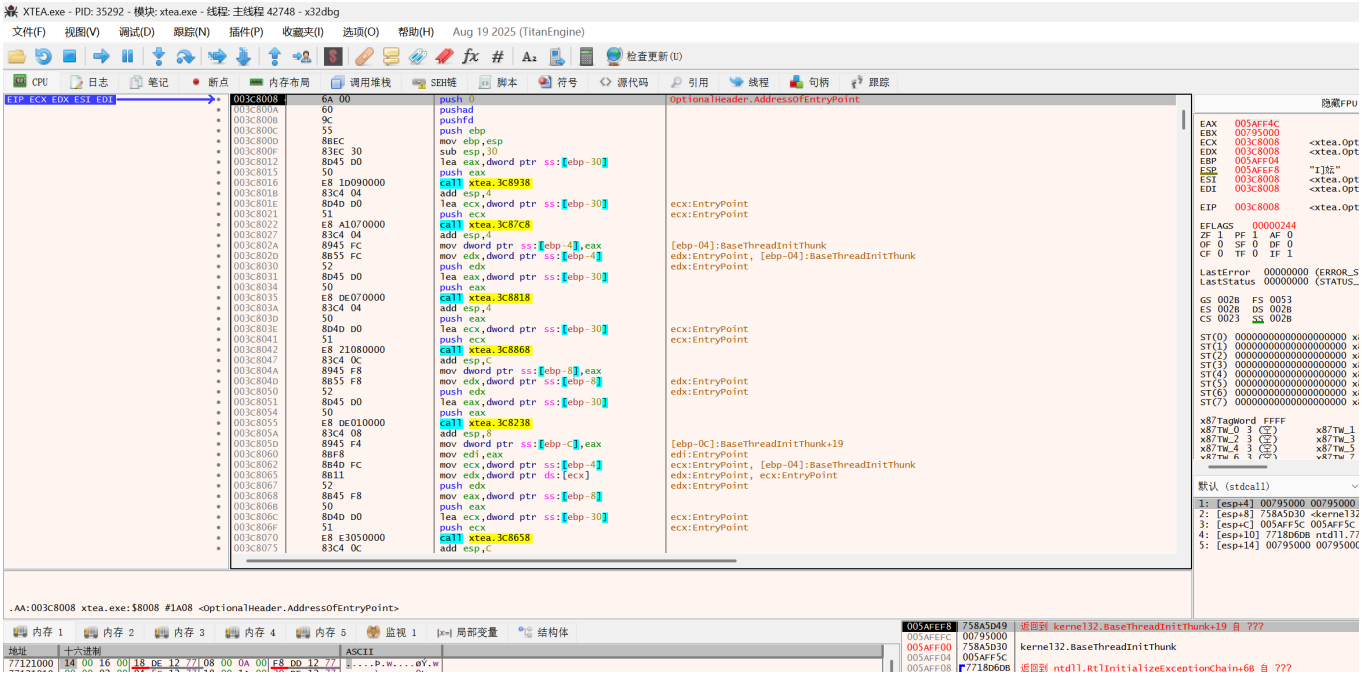
逆向wp-7

逆向题目wp

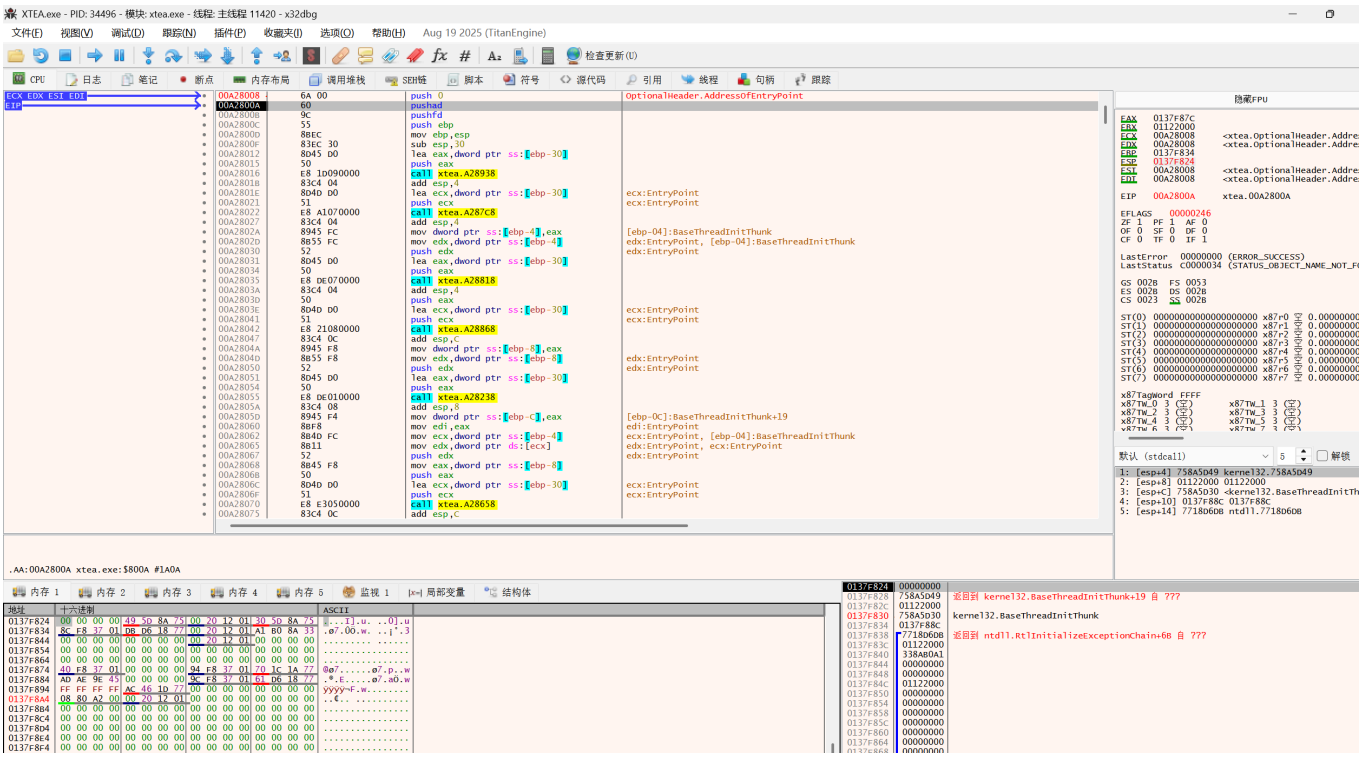
张程思

一,xtea(复现一下这次isctf没解出来的一个题)

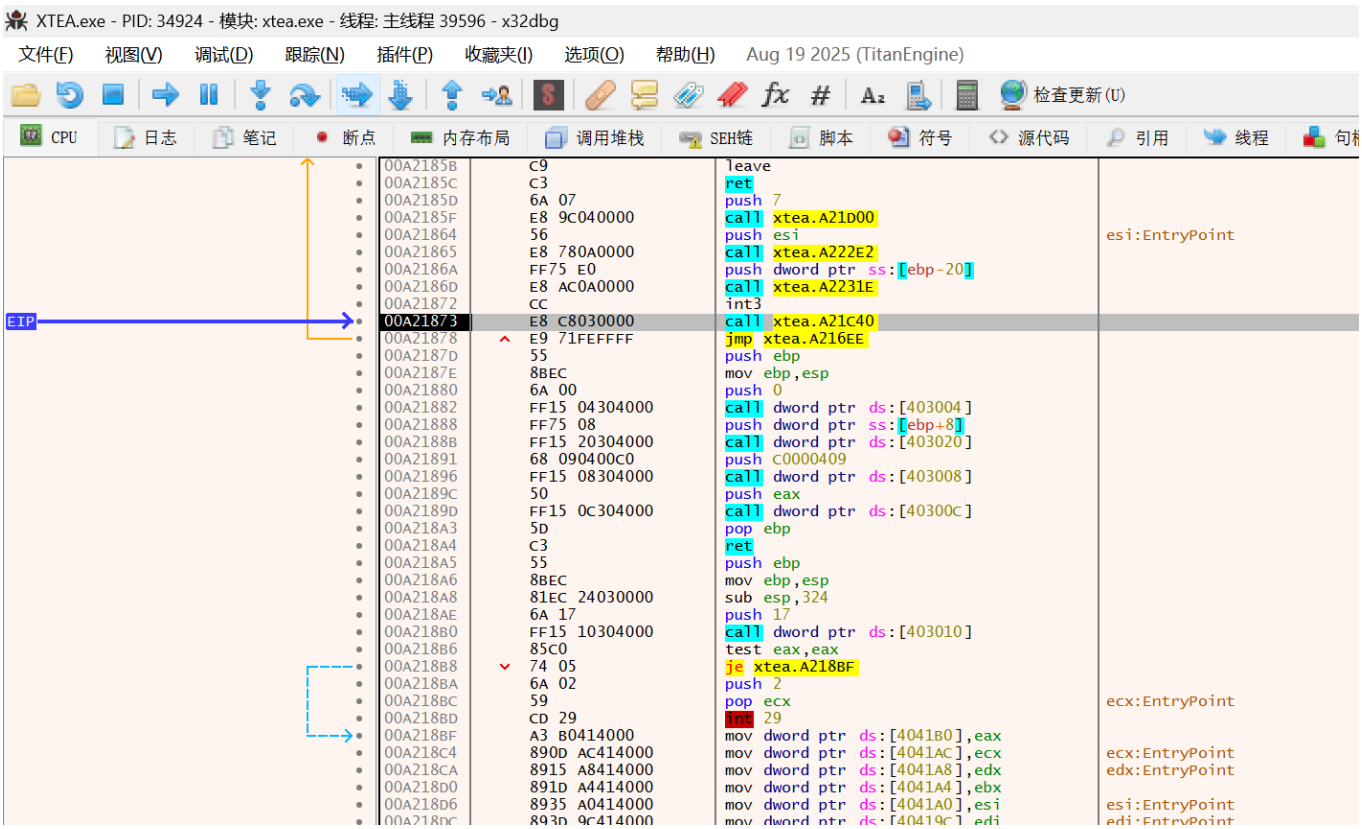
1,这个是一个程序带有一个别人的手搓壳,先x32dbg打开,用esp定律脱第一步,先f9跳到这里



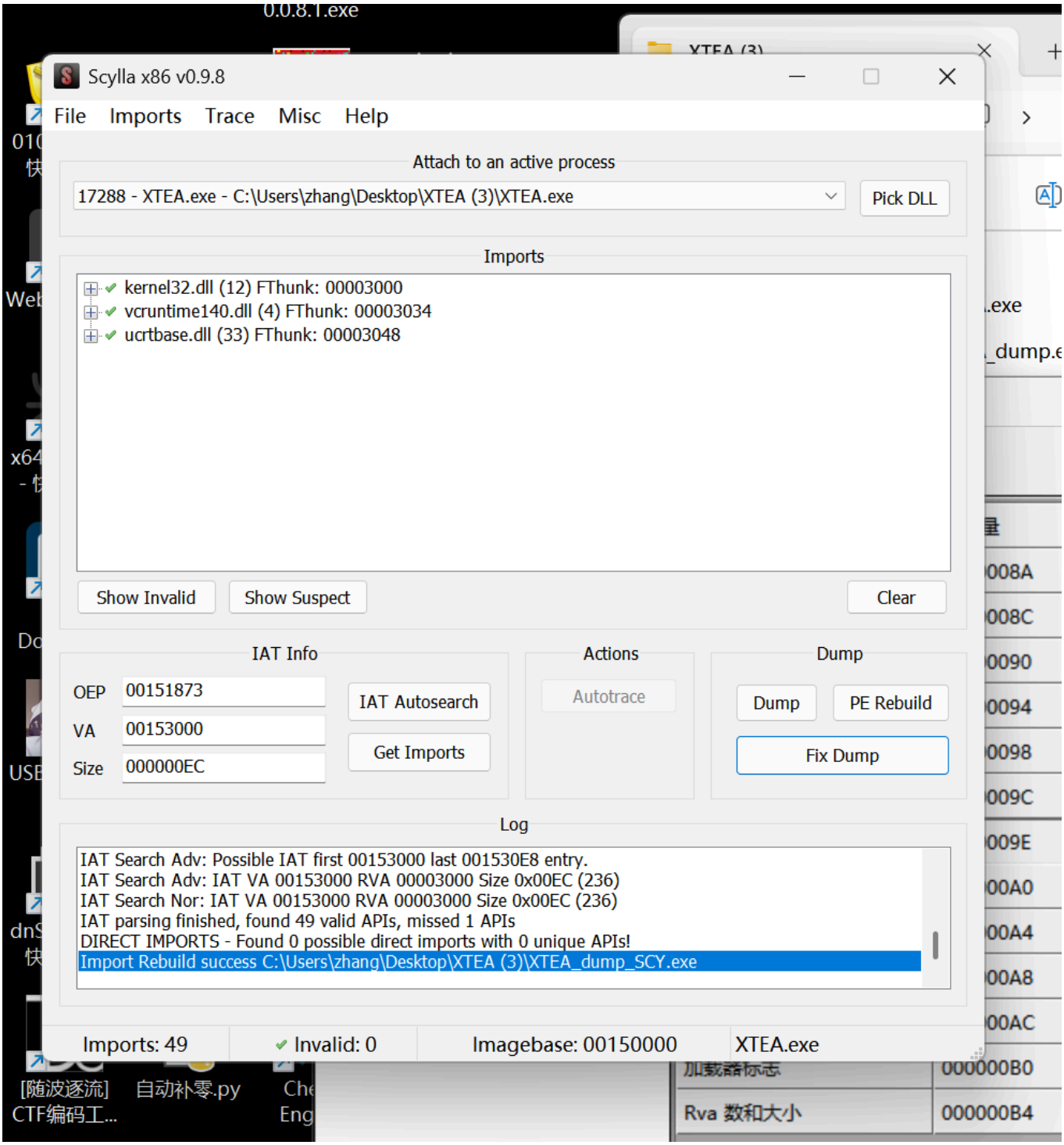
2,下个断点



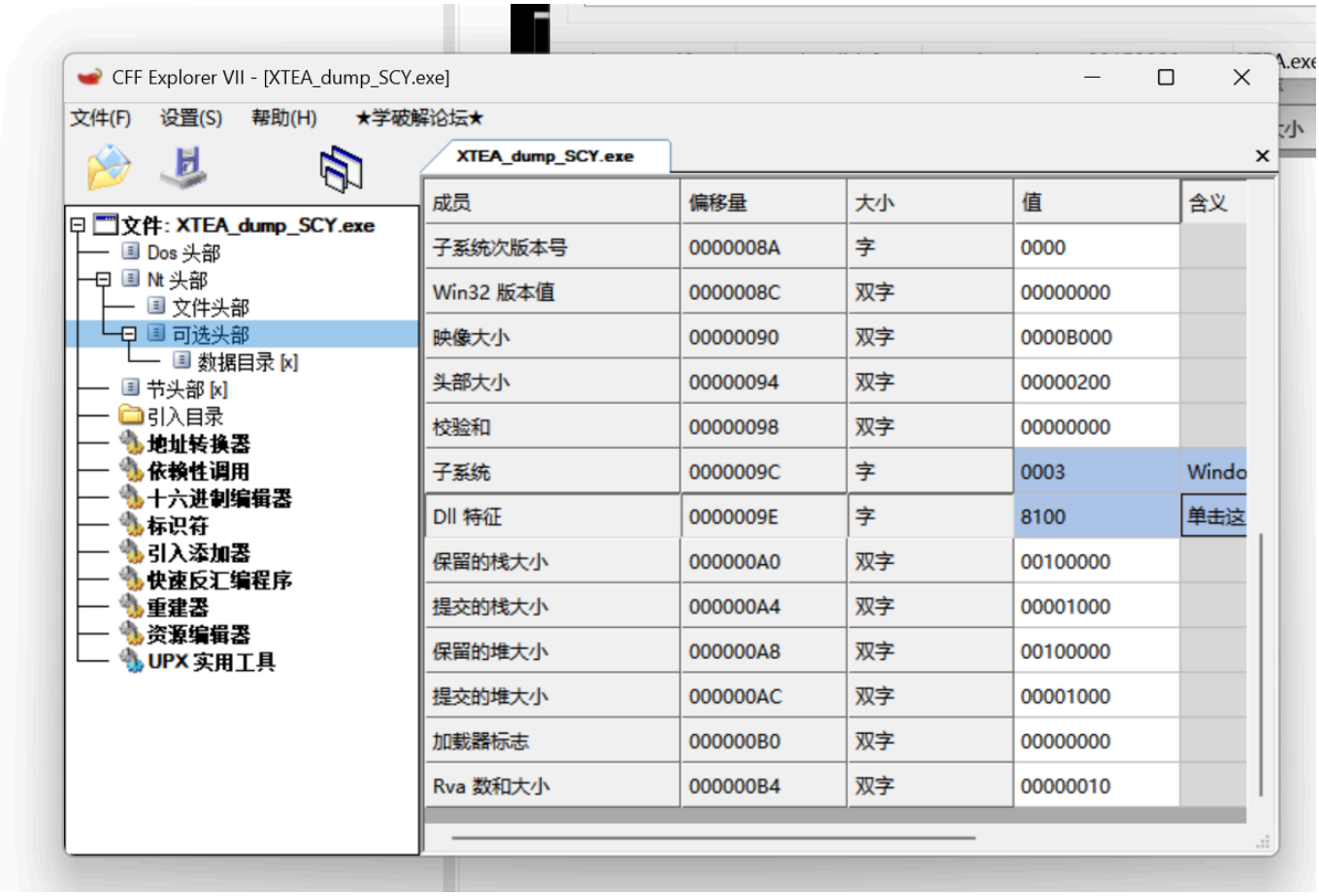
3,跳到这里dump



4,fixdump一下



5,再用cff去除重定位



6,终于能打开了!

剩下的很简单了,就是xtea算法加密解密