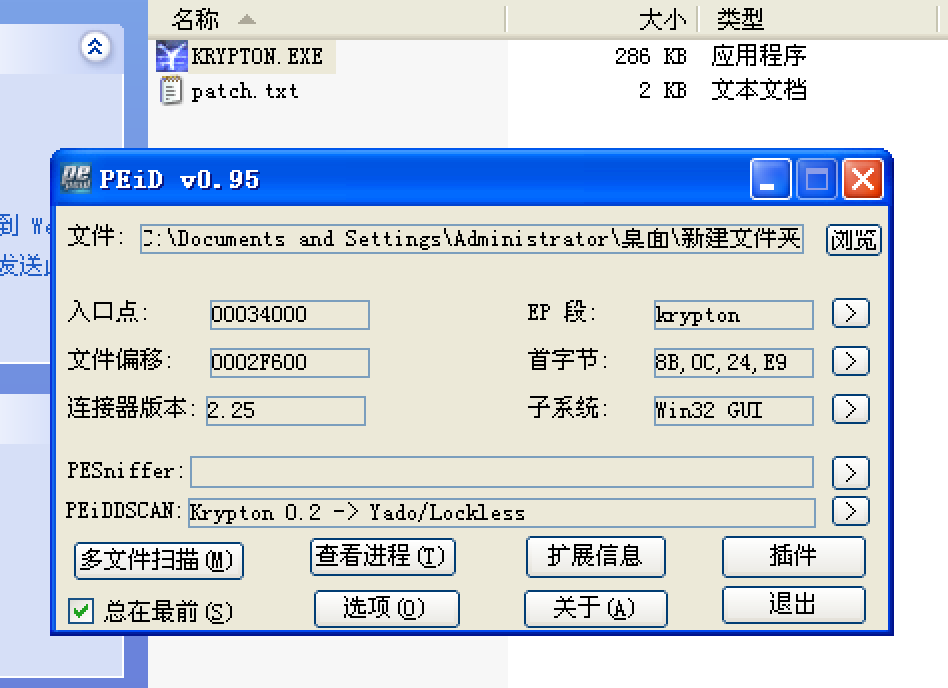
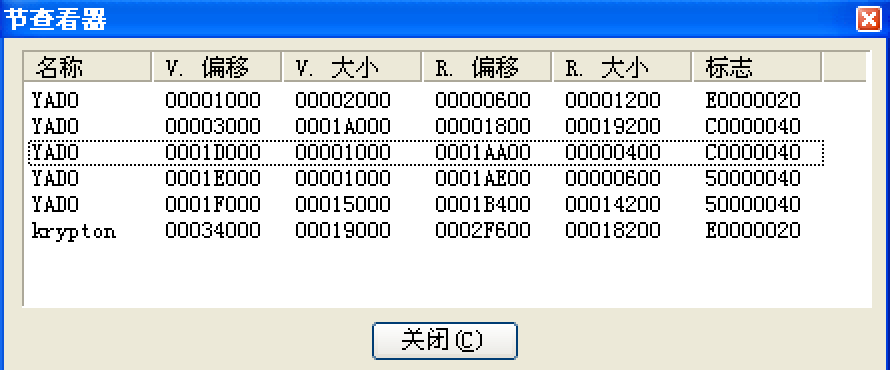
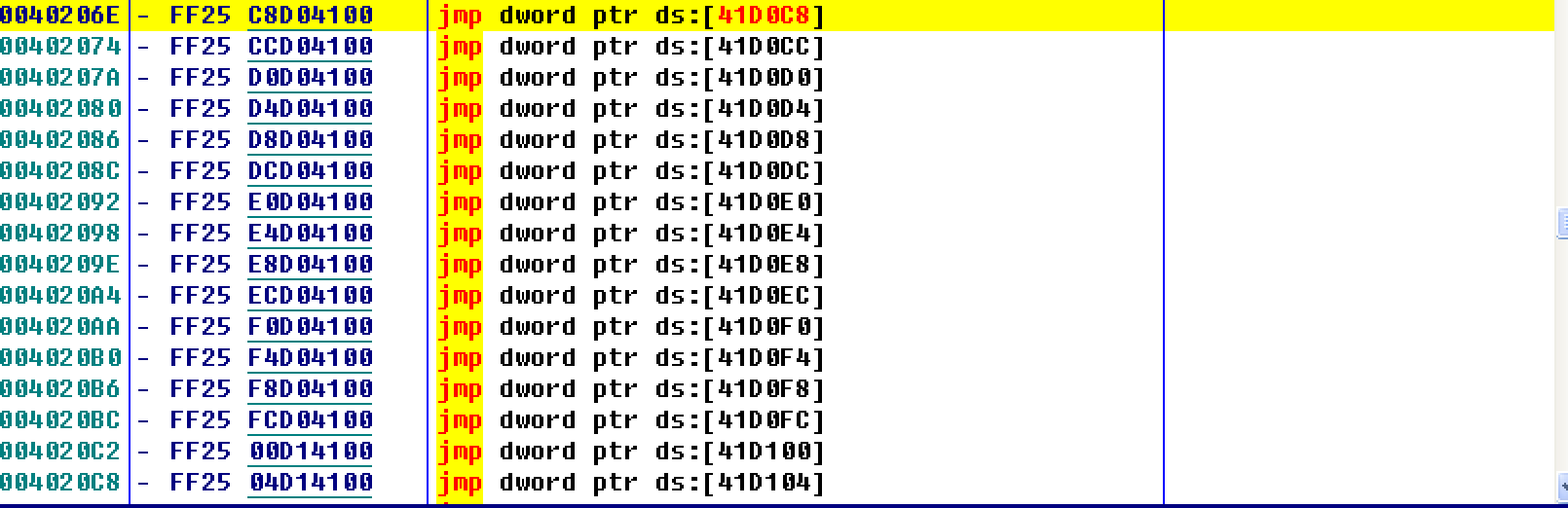
样本就是他自己，自己给自己加壳了。可以用patch，脱使用他加密过的PE壳

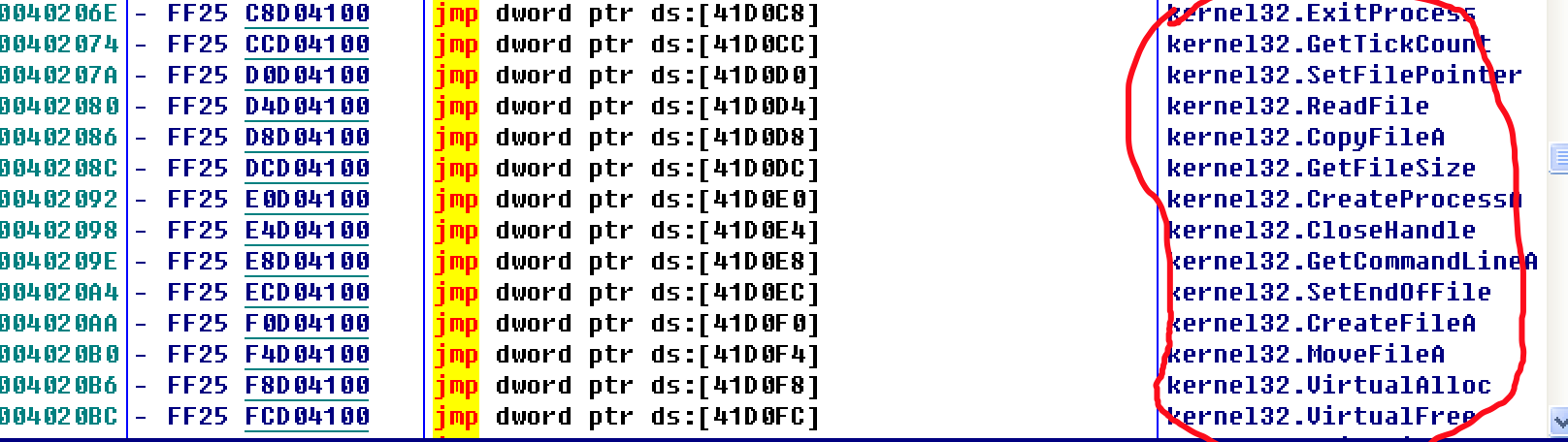




运行patch前，导入表时加密过的：



运行patch解密之后：



导入表信息已经被解密出来了。修复之后，可以正常运行，查看PE信息显示编译环境为TASM32：

