Week 2

Re

xD MAZE
upx magic 0
fake shell
creakme2
upx magic1

xD MAZE

迷宫题，把题拖进IDA里面F5看main函数，看下迷宫怎么“走”，根据“failed“和“length err”找到判断条件判断“往哪走”即可解题。

上代码：）(代码不是特别严谨dbq)

```
#include<stdio.h>
int main(void)
{
    int a[4096] =
    {
      32,
      32,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
      35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
            35,
            32,
            32,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
            35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        32,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
        35,
      35,
      35,
      35,
      35,
      32
    };
    int b[1000] = { 1 };
    int k = 0;
    int c[100]={1};
    char flag[50] = { 8 };
    for (int i = 0; i < 4096; i++)
    {
        if (a[i] == 32)
        {
            b[k] = i;
            k++;
        }
    }
    for (int i = 0; i < 99; i++)
    {
        c[i] = b[i + 1] - b[i];
        switch (c[i])
        {
        case 512:
            flag[i] = '0';
            break;
        case 64:
            flag[i] = '1';
            break;
        case 8:
            flag[i] = '2';
            break;
        case 1:
            flag[i] = '3';
        default:
            continue;
        }
    }
    for (int i = 0; i < 1000; i++)
    {
        printf("%c", flag[i]);
    }
    return 0;
}
```

upx magic 0

（虚假的upx:()

拖进IDA然后F5然后shift+F12快速找到main函数，发现是个不可逆的算法（CRC16算法【一种信息摘要算法】），爆破解决

上代码：）

```
#include<stdio.h>
```

```
int main(void)
{
    int v10[32];
    v10[0] = 36200;
    v10[1] = 40265;
    v10[2] = 10770;
    v10[3] = 43802;
    v10[4] = 52188;
    v10[5] = 47403;
    v10[6] = 11826;
    v10[7] = 40793;
    v10[8] = 56781;
    v10[9] = 40265;
    v10[10] = 43274;
    v10[11] = 3696;
    v10[12] = 62927;
    v10[13] = 2640;
    v10[14] = 23285;
    v10[15] = 65439;
    v10[16] = 40793;
    v10[17] = 48395;
    v10[18] = 22757;
    v10[19] = 14371;
    v10[20] = 48923;
    v10[21] = 30887;
    v10[22] = 43802;
    v10[23] = 18628;
    v10[24] = 43274;
    v10[25] = 11298;
    v10[26] = 40793;
    v10[27] = 23749;
    v10[28] = 24277;
    v10[29] = 30887;
    v10[30] = 9842;
    v10[31] = 22165;
    int flag[32];
    for (int i = 0; i < 37; i++)
    {
        for (int k = 0; k < 0x7F; k++)
        {
            flag[i] = k;
            flag[i] = flag[i] << 8;
            for (int j = 0; j <= 7; ++j)
            {
                if ((flag[i] & 0x8000) != 0)
                {
                    flag[i] = (2 * flag[i]) ^ 0x1021;
                }
                else
                {
                    flag[i] *= 2;
                }
            }
            flag[i] = (unsigned __int16)flag[i];
            if (flag[i] == v10[i])
            {
                putchar(k);
                break;
            }
        }
    }
    return 0;
}
```

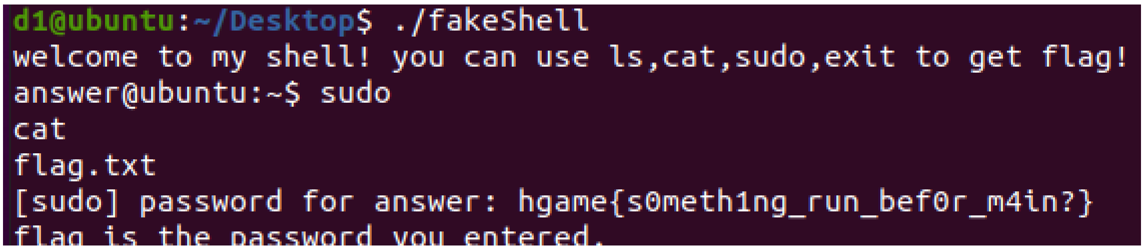
fake shell

拖进IDA然后F5反编译，分析一下发现需要找到password，找到加密函数发现是RC4算法，但是解密发现不对，根据学长的hint还有观察发现密钥在某个隐秘的地方偷偷换了0v0，处理一下数据再拖进CyberChef解密就能得到flag啦！不对，就能得到password啦！然后在Linux上运行一下发现——

处理数据^v^

```
#include<stdio.h>
int main(void)
{
    long long v[4];
    v[0] = 0xE0B25F3D8FFA94B6LL;
    v[1] = 0xE79D6C9866D20FEALL;
    v[2] = 0x6D6FBEC57140081BLL;
    v[3] = 0xF6F3BDA88D097B7CLL;
    char* flag = (char*)v;
    for (int i = 0; i < 32; ++i)
    {
        printf("%x ", flag[i]&0xFF);
    }
}
```

打开文件^v^"



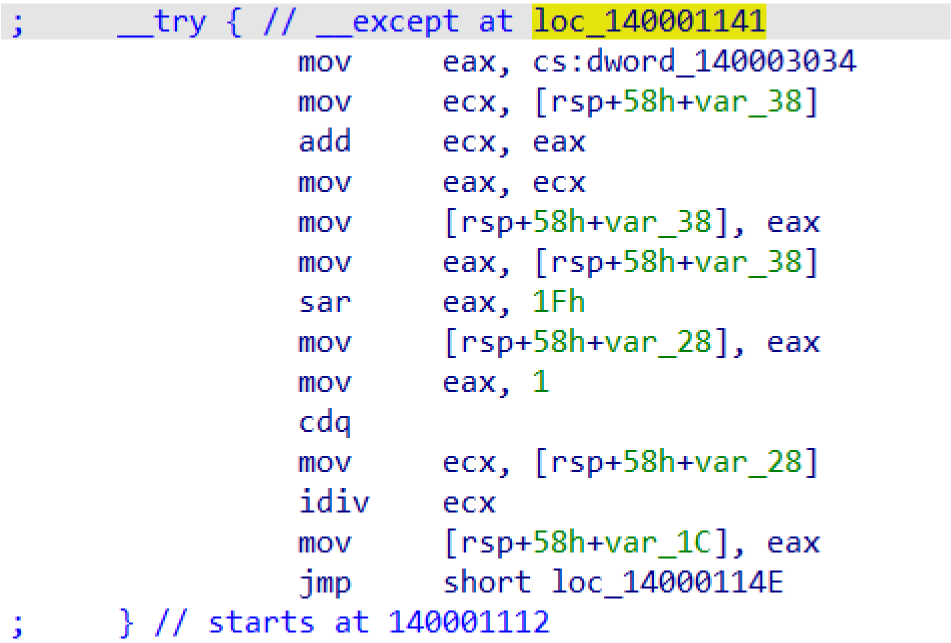
```
d1@ubuntu:~/Desktop$ ./fakeShell
welcome to my shell! you can use ls,cat,sudo,exit to get flag!
answer@ubuntu:~$ sudo
cat
flag.txt
[sudo] password for answer: hgame{s0meth1ng_run_bef0r_m4in?}
flag is the password you entered.
```

hhh

creakme2

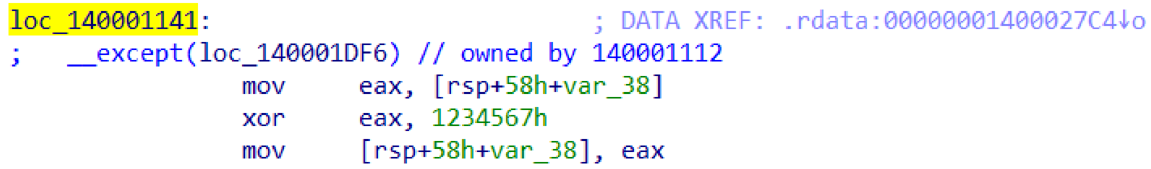
根据学长的hint了解Windows SEH异常处理机制，IDA会将这一部分的代码优化导致F5之后main函数不会包括这一段的反编译代码，所以在汇编中找到try块的位置,except的位置以及except()里的位置，当时学习的时候参考了一下一个用简单的_try语法写的小程序拖进IDA里面大概是什么样的，【这里要注意一下拖进去的小程序在vs2022中编译选项为x64release】从而能更清晰地分析每个块中的汇编对应的内容。

先分析第一个try块，反编译一下发现是对主函数中加密函数的一个变量（这里暂且记作v4）进行处理



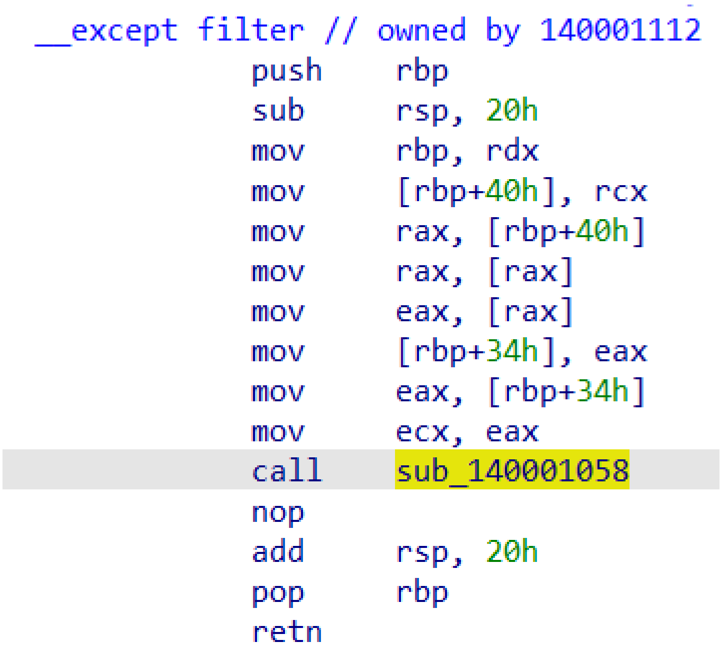
```
;       __try { // __except at loc_140001141
                mov     eax, cs:dword_140003034
                mov     ecx, [rsp+58h+var_38]
                add     ecx, eax
                mov     eax, ecx
                mov     [rsp+58h+var_38], eax
                mov     eax, [rsp+58h+var_38]
                sar     eax, 1Fh
                mov     [rsp+58h+var_28], eax
                mov     eax, 1
                cdq
                mov     ecx, [rsp+58h+var_28]
                idiv    ecx
                mov     [rsp+58h+var_1C], eax
                jmp     short loc_14000114E
;       } // starts at 140001112
```

根据注释找到对应的except块



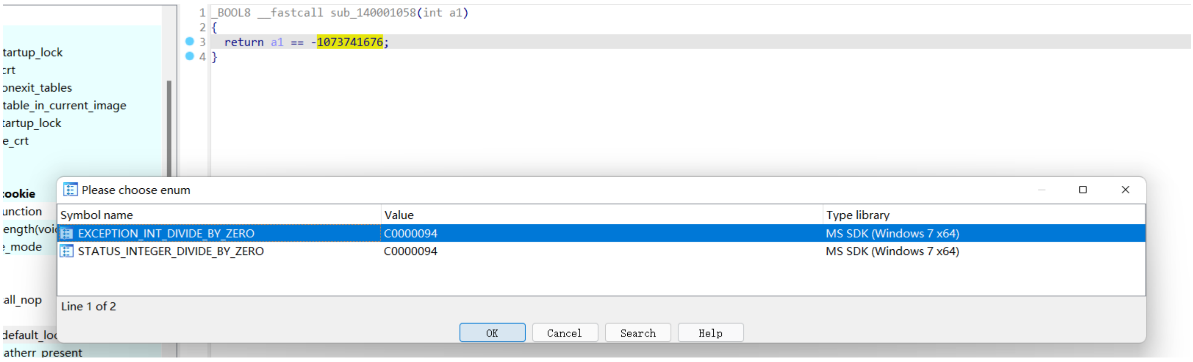
```
loc_140001141:                          ; DATA XREF: .rdata:00000001400027C4↓o
;   __except(loc_140001DF6) // owned by 140001112
                mov     eax, [rsp+58h+var_38]
                xor     eax, 1234567h
                mov     [rsp+58h+var_38], eax
```

在括号中找到过滤块



```
__except filter // owned by 140001112
                push    rbp
                sub     rsp, 20h
                mov     rbp, rdx
                mov     [rbp+40h], rcx
                mov     rax, [rbp+40h]
                mov     rax, [rax]
                mov     eax, [rax]
                mov     [rbp+34h], eax
                mov     eax, [rbp+34h]
                mov     ecx, eax
                call    sub_140001058
                nop
                add     rsp, 20h
                pop     rbp
                retn
```

进call反编译



```
_BOOL8 __fastcall sub_140001058(int a1)
{
  return a1 == -1073741676;
}
```

Please choose enum

Symbol name	Value	Type library
EXCEPTION_INT_DIVIDE_BY_ZERO	C0000094	MS SDK (Windows 7 x64)
STATUS_INTEGER_DIVIDE_BY_ZERO	C0000094	MS SDK (Windows 7 x64)

Line 1 of 2

m键让IDA标记为有意义的枚举常量，发现该异常是除零异常，再返回try块中的汇编代码分析过程，过程大概就是1/(v4>>31)，当三十二位的int右移三十一位后剩下最左边的一位，它为零时就会触发除零异常，从而进行except块中的异常处理，即异或0x1234567

还有一个整块用相同的办法分析出来是栈溢出异常处理，但是动态调试一下发现程序没有触发该异常，所以可以不用管它），将过程结合XTEA加密算法解密，上代码>"<

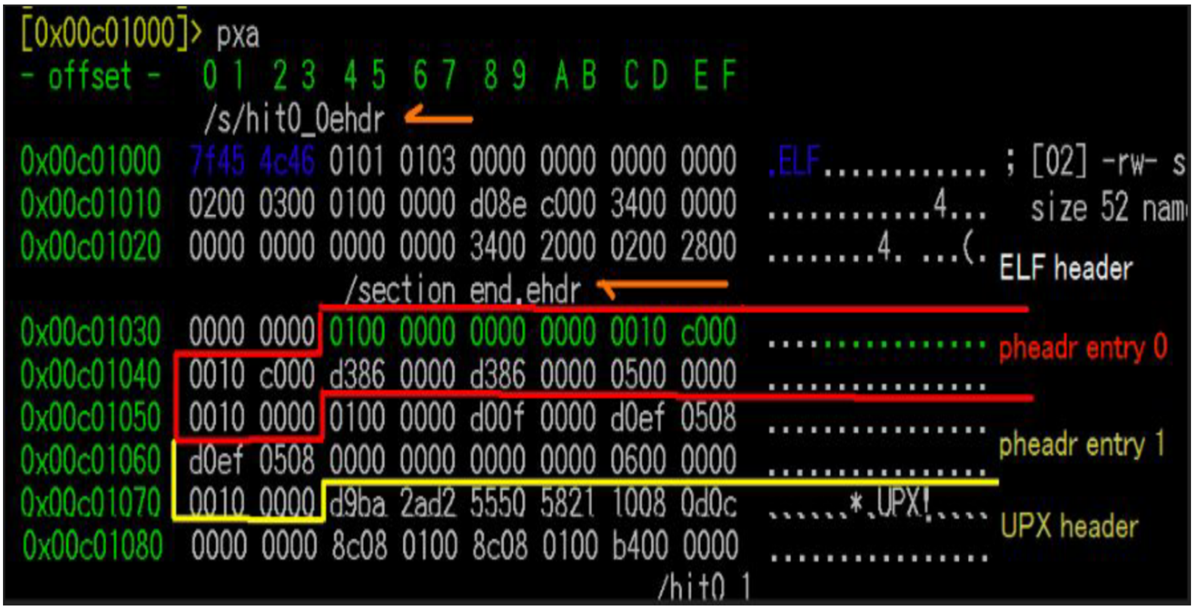
```
#include<stdio.h>
#include<iostream>
void decipher(unsigned int num_rounds, uint32_t v[2], uint32_t const key[4]) {
    unsigned int i;
    uint32_t v0 = v[0], v1 = v[1], delta = 0x9E3779B1;
    uint32_t sum = 0xc78e4d05;//注意一下这个地方的sum值，可以加密一次相同过程获得
    for (i = 0; i < num_rounds; i++) {
        v1 -= (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum >> 11) & 3]);
        if ((sum >> 31) == 0)
        {
            sum ^= 0x1234567;
        }
        sum -= delta;
        v0 -= (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum + key[sum & 3]);
    }
    v[0] = v0; v[1] = v1;
}
int main(void)
{
    unsigned int v5; // [rsp+24h] [rbp-34h]
    unsigned int v6; // [rsp+28h] [rbp-30h]
    int v11[10];
    int Buf2[8];
    v11[9] = 0;
    v11[0] = 1;
    v11[1] = 2;
    v11[2] = 3;
    v11[3] = 4;
    v11[4] = 5;
    v11[5] = 6;
    v11[6] = 7;
    v11[7] = 8;
    v11[8] = 9;
    Buf2[0] = 0x457E62CF;
    Buf2[1] = 0x9537896C;
    Buf2[2] = 0x1F7E7F72;
    Buf2[3] = 0xF7A073D8;
    Buf2[4] = 0x8E996868;
    Buf2[5] = 0x40AFAF99;
    Buf2[6] = 0xF990E34;
    Buf2[7] = 0x196F4086;
    decipher(32, (uint32_t*)Buf2, (uint32_t*)v11);
    decipher(32, (uint32_t*)(Buf2+2), (uint32_t*)v11);
    decipher(32, (uint32_t*)(Buf2+4), (uint32_t*)v11);
    decipher(32, (uint32_t*)(Buf2+6), (uint32_t*)v11);
    char* flag = (char*)Buf2;
    for (int i = 0; i < 32; i++)
    {
        printf("%c", flag[i]);
    }
}
```

upx magic1

真正的upx！但是发现是个变形的壳OvO（可以根据upx -d报错来判断？）

那就把它改回来：）参考了一下0w1学姐的博客

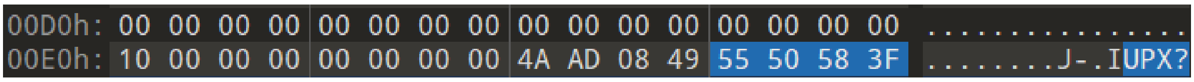
upx文件头结构



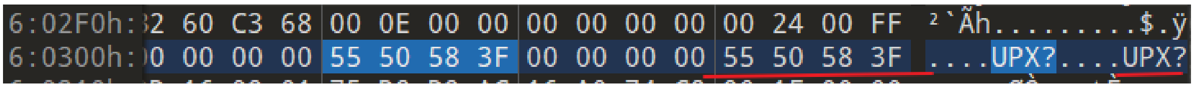
```
[0x00c01000]> pxa
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F
               /s/hit0_0ehdr
0x00c01000  7f45 4c46 0101 0103 0000 0000 0000 0000  .ELF............  ; [02] -rw- s
0x00c01010  0200 0300 0100 0000 d08e c000 3400 0000  ............4...   size 52 nam
0x00c01020  0000 0000 0000 0000 3400 2000 0200 2800  ........4. ...(.
                      /section end.ehdr
0x00c01030  0000 0000 0100 0000 0000 0000 0010 c000  ................
0x00c01040  0010 c000 d386 0000 d386 0000 0500 0000  ................
0x00c01050  0010 0000 0100 0000 d00f 0000 d0ef 0508  ................
0x00c01060  d0ef 0508 0000 0000 0000 0000 0600 0000  ................
0x00c01070  0010 0000 d9ba 2ad2 5550 5821 1008 0d0c  ......*.UPX!....
0x00c01080  0000 0000 8c08 0100 8c08 0100 b400 0000  ................
                                          /hit0_1
```

复原：）

拖进010 Editor里面把下图选中区域都改成upx就可以upx -d了！



```
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00E0h: 10 00 00 00 00 00 00 00 4A AD 08 49 55 50 58 3F  ........J-.IUPX?
```



```
6:02F0h:32 60 C3 68 00 0E 00 00 00 00 00 00 00 24 00 FF  ²`Ãh........$.ÿ
6:0300h:00 00 00 00 55 50 58 3F 00 00 00 00 55 50 58 3F  ....UPX?....UPX?
```

跟虚假的upx基本相同的解密过程)

```
v14={}
v14[0]=36200
v14[1]=40265
v14[2]=10770
v14[3]=43802
v14[4]=52188
v14[5]=47403
v14[6]=11826
v14[7]=40793
v14[8]=56781
v14[9]=40265
v14[10]=43274
v14[11]=3696
v14[12]=62927
v14[13]=24277
v14[14]=15363
v14[15]=31879
v14[16]=9842
v14[17]=43802
```

```
v14[18]=2640
v14[19]=23285
v14[20]=65439
v14[21]=40793
v14[22]=48395
v14[23]=22757
v14[24]=14371
v14[25]=48923
v14[26]=30887
v14[27]=43802
v14[28]=18628
v14[29]=43274
v14[30]=11298
v14[31]=40793
v14[32]=23749
v14[33]=24277
v14[34]=30887
v14[35]=9842
v14[36]=22165
flag={}
for i in range(37):
  for k in range(127):
    flag[i]=k
    flag[i] = (flag[i] << 8)&0xffff
    for j in range(8):
      if((flag[i]&0x8000)!=0):
        flag[i]=(2*flag[i])^0x1021
      else:
        flag[i]*=2
    flag[i]=(flag[i]&0xffff)
    if(flag[i]==v14[i]):
      print(chr(k),end="")
```