1. 用IDA打开exe文件
2. ebp指向当前帧底部(地址大)

esp指向当前帧顶部（地址小）

1. 找到main函数，和其中定义在栈帧中的局部变量，通过它们地址连续并以char类型结尾，推测出为字符串。
2. 每个int类型数据为4个字节，即表示4个字符，每个int类型数据里按从小地址到大地址的顺序翻译为4个字符，最终组合出



1. 根据复原代码的逻辑，当输入字符串=硬编码在软件里的

时，循环中止，程序打印成功，结束运行。