ida属于逆向分析中的静态分析，通过看汇编代码，F5插件比较好用，把伪代码还原成代码。

动态分析，windows是，linux是。

elf在linux可执行文件。windows下是exe和dll。

ascll编码，编码和解码。

导入表

PE文件结构

exe dll 运行的时候 会从外部调用一些函数

加壳？

如果有壳 只有两个函数 Loadlibrary（） ---

反汇编代码 得到的函数较少

软件：我爱破解

ollydebug 动态调试

标志寄存器 Z 1 计算结果为0 ……

快捷键 F8 单步执行 F7 步入

win32 窗口程序

win32 控制台程序

区别：窗口程序有一个消息循环

windows操作系统：消息机制

消息循环

对一些特定的函数下断点

windows程序设计

从输入框获取输入：GetWindowText（） GetDlgItem（）

-A

apk zip解压 classes.dex 用dex2jar 转变成java包 JD-GUI读java包

