PC端方向分为初赛和复赛两个阶段。

每个阶段均有ring0和ring3两道题，每个阶段得分为ring0题与ring3题得分之和。

初赛和复赛分别记分，相互独立，复赛选手的复赛得分，与初赛得分无关。

根据题目要求，需要提供文档或源代码，推荐使用文本文件、Word文档、pdf格式。

**答案压缩包的命名格式为: 决赛-PC客户端-姓名-学校-联系电话.zip**

决赛共分为ring3和ring0两道题，分别是5分和10分，累计积分，满分15分。

复赛ring3题目：（本题共5分）

winmine.exe是一个扫雷游戏程序，winmine.dmp是该程序的一份进程dump, 在这份dump中，有一个DLL作弊程序。

1, 请找到该作弊程序，给出模块名；（1分）

2, 并分析它所包含的4个作弊功能，给出实现作弊功能的函数的偏移，并说明其作弊功能是什么。（4分）

复赛ring0题目：（本题共10分）

本题分为2个部分，共10分，每部分总计5分。驱动加载环境为WIN10（推荐1803~1903范围内的系统）。

Part1：

(1) 成功加载Driver.drv至驱动模块链表（0.5分）

(2) 自编写驱动加载程序，使用非服务方式加载Driver.drv驱动，加载后需要保证驱动路径为C:\Driver.drv（0.5分）

(3) 分析驱动接口，给出每个功能的调用控制码，输入，输出数据的结构（0.5分）

(4) 分析驱动接口，分析每个接口的作用（0.5分）

(5) 调用驱动接口，使Driver.drv在驱动模块中断链隐藏（只允许在应用层调用Driver.drv接口实现）（2分）

(6) 从Flag.fg中分析出Flag，此flag用于解密Part2.7z（1分）

以详细文档、源代码、构建好的bin的方式提供答案。

Part2：

运行RunGame.bat将启动一个游戏demo, 以管理员权限运行外挂程序DemoEsp.exe, 外挂程序将对游戏产生透视效果。

请编写驱动程序阻止外挂透视行为，按照符合以下(1)~(5)的条件限制来给分。

按照反外挂的思路实现，不可直接攻击外挂进程（例如结束进程、结束线程等），可从内存/文件/绘制等方面入手。

(1) 在未开启外挂的情况下游戏正常运行；

开启外挂后，游戏也正常运行；

开启游戏，开启外挂，开启编写的驱动程序后，游戏正常运行，但是外挂失效；（1分）

(2) 该驱动程序可以做到，非句柄回调保护，非句柄降权，非特征码定位，非文件样本；（1分）

(3) 该驱动程序可以做到，非内核函数代码段hook; （1分）

(4) 可以运行在WIN10 X64（1909-20H1范围）；（1分）

(5) 可以兼容（1903~20H1范围）内的HVCI. （1分）

以详细文档、源代码（part2可选，建议提供）、构建好的bin的方式提供答案。