1. **形成分组，每组6-7人，选出组长，提交分组名单，标出组名、组长及成员：**

组名：detours.h :

成员：郭记宏，范方耀，吴锦添，尚世权，杨永灿，李泽伟

组长：李泽伟

1. **学习Detours资料（见附件1指导手册文档 2微软官网第一篇相关文章），理解该方法注入WindowsAPI的流程，小组内讨论自己关于课设要求的理解及初步完成安排；组长主持下，成员轮流发言，组内成员对发言人进行评价。并记录自己完成课设的初步安排。**

我对于注入WindowsAPI的流程理解：

在Detours库的帮助下，使用DetourAttach()函数截获所设定的WindowsAPI，同时定义相应的New函数来完成函数流的转移，这样就可以截获到WindowsAPI的相应参数信息，同时让指令流跳转到自己设定的函数，在这个函数中打印出截获的参数信息。而后再使用DetourDetach()函数取消对该API的截获。

我对于课设要求的理解和初步安排：

在认真查看完老师所给的指导手册文档后，实际上对于Detours的几个基本函数已经有了粗略的一些了解，对于课设所给予的任务也有相应的一点点感觉，哪些比较易于实现，哪些是比较困难的。个人感觉前六个任务都是比较容易实现的，由于对于注册表的操作没有接触过，感觉任务七可能会花比较长的时间。选做的任务10，小组成员觉得在上学期所学的计算机网络实验的基础上是相对其他选做任务容易实现一些的。

所以我的任务安排是：第一周完成前六个任务，后续的必做任务在第二周完成，同时争取完成选做任务10，如果时间还有富裕的话，可以再尝试完成选做任务11。

我对其他组员的评价：

郭记宏：讲述了自己的一些理解和任务规划。 评分：99

范芳耀：讲述了自己在实验中的一些问题和想法。 评分：99

吴锦添（我自己 不做评价）

尚世权：讲述了自己的一些理解和任务规划。 评分：99

杨永灿：对于dll文件生成有一些独特的理解。 评分：99

李泽伟：讲述了自己的一些理解和任务规划。 评分：99

1. **完成Detours源码编译、VS环境配置准备**

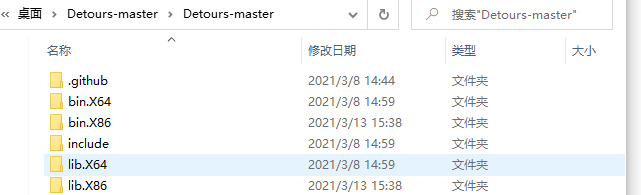


图3.1 Detours源码编译

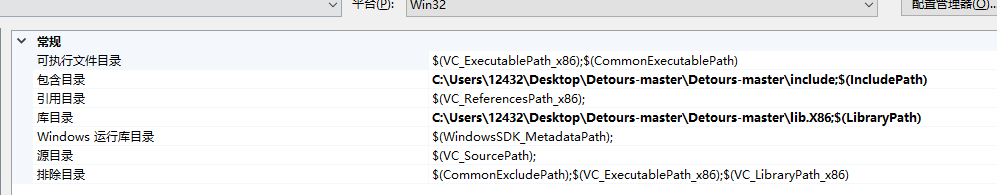


图3.2 VS编译环境配置

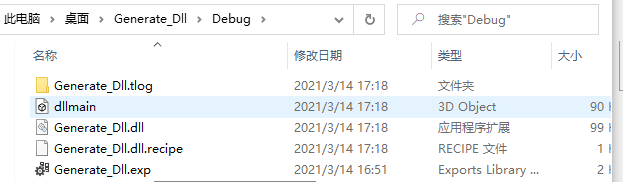


图3.3 dll文件的生成

1. **完成简单注入样例（可选）**

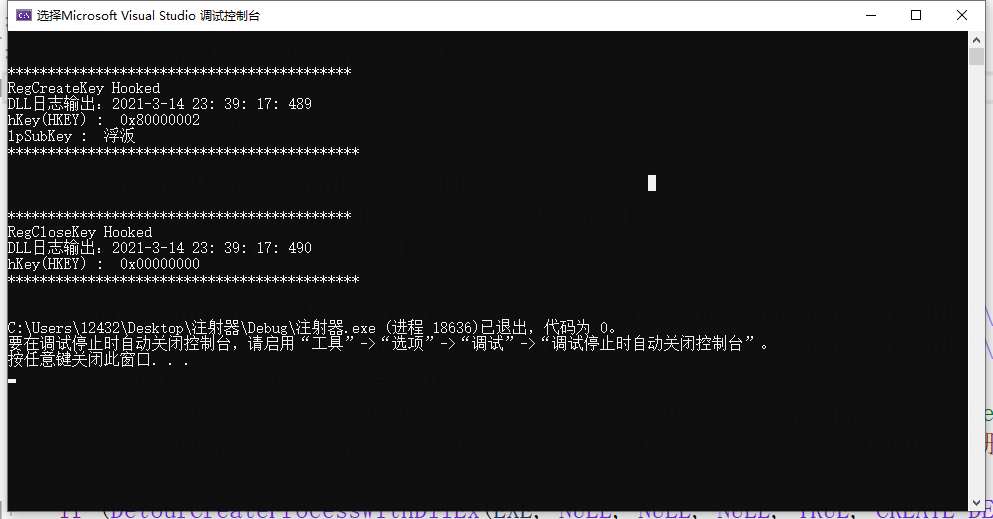


图4.1 对注册表的截获

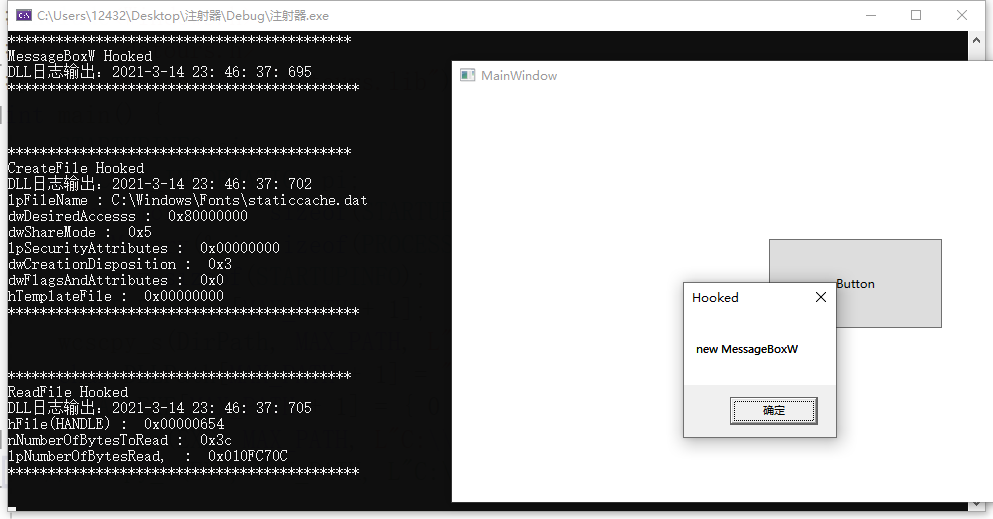


图4.2 对弹窗的截获

1. **编写DLL工程及搭建框架**

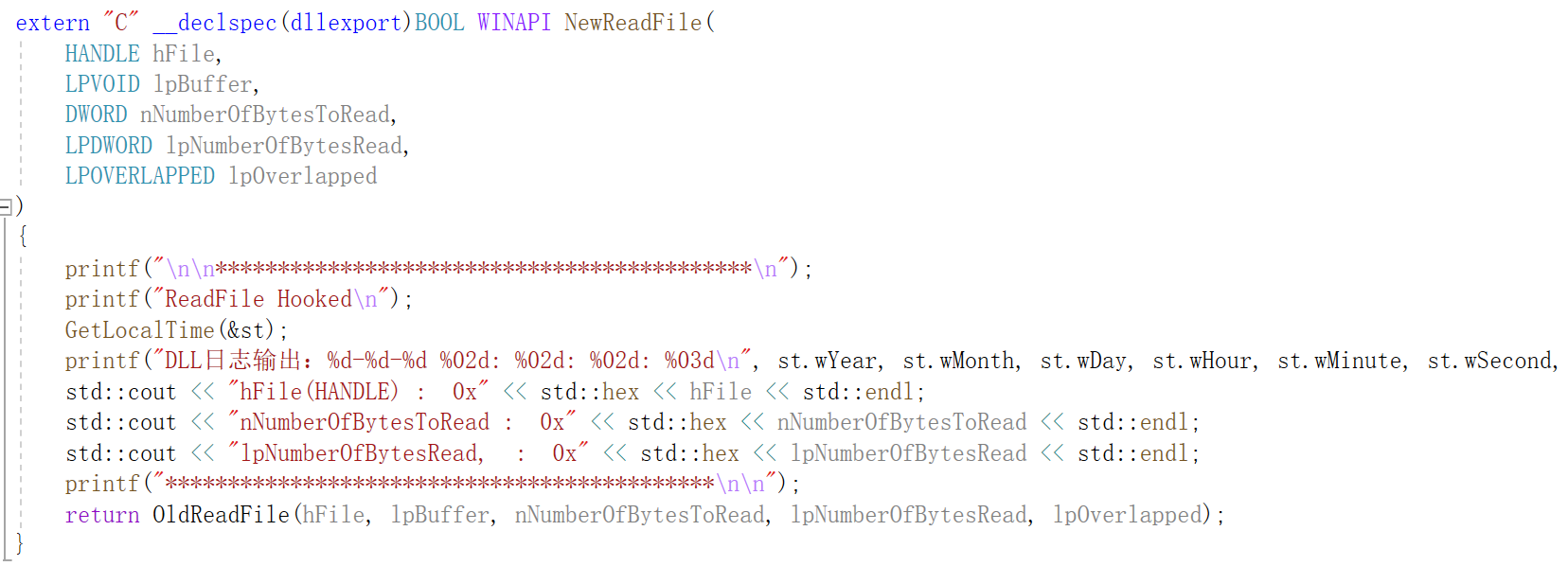


图5.1 ReadFile的截获



图5.2 DllMain函数的定义