1. **本次课设需要虚拟机靶机吗？**

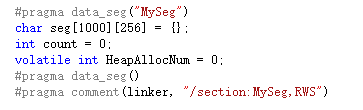
答：本次课设完全可以基于Win10，VS2019开发，不用安装虚拟机。

1. **printf怎么没看到输出信息呢？**

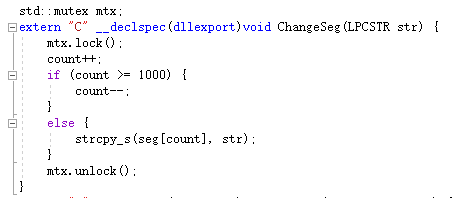
答：Dll中的printf语句在被注入的进程中运行，如果被注入的进程不是控制台程序，就无法输出。建议：

1.使用OutputDebugString输出调试语句，用Dbgview.exe查看该函数的输出；

2.在Dll中设置一个进程间共享缓冲区，所有输出放入该缓冲区，注射程序通过读取该缓冲区获得调试输出：



注意做好数据操作的互斥操作：



1. **指导书中的代码都是正确的吗？**

答：指导书前面部分的代码是针对VC6的代码,使用的Detours版本比较低，在VS2019编译无法通过，请参照指导书中最后的代码。注意该代码可以完成基本的MessageBoxA/W截获，主要是大家参考其基本运行原理。在扩大到其它API的时候，请仔细检查代码，遇到问题单步跟踪，排除问题。

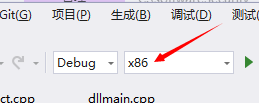
1. **我发现有截获API输出信息比预想要多的多，陷入死循环了，怎么办？**

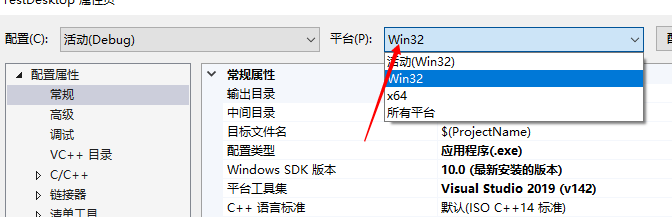
答：可能有两个原因：

1是注射器程序自身加载了Dll，导致自身的API被截获了，输出了意外的截获信息，建议在DllMain里面判断一下是否为注射器程序自身，如果是，则不要开启Detours的API截获。比如可以通过GetModuleFileName(0, Buf, 256)得到当前进程名，比较判断是否为注射器名字即可。

2.截获的API存在重入的问题，部分函数存在递归调用。导致输出无穷无尽。比如:可能在自己定义的HeapAlloc的截获函数中使用了printf,但printf函数实现中，使用了HeapAlloc,又被截获下来，这样就进入了无穷递归了。建议1.判断自己定义的HeapAlloc函数是否被重入，如果被重入，直接调用原始HeapAlloc直接返回，不要输出即可。 2.更改输出方式，避免重入函数的调用。

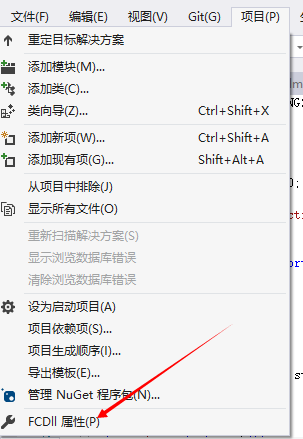
1. **我明明设置了包含目录(将inlcude目录加入Detours的include文件夹所在的路径)，也将库文件所在的目录加入，但为什么还是编译提示没有定义或者函数没有定义？**

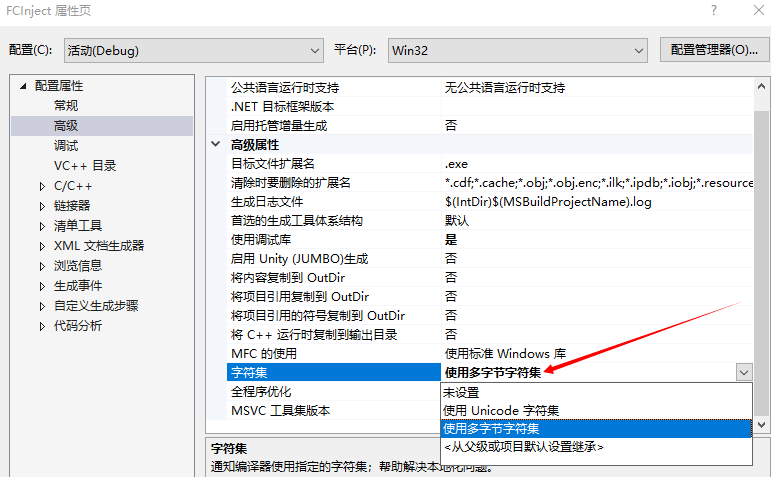
答：注意我们的实例代码是针对x86，注意检查编译目标是不是x86，不要选为x64,类似在配置项目的包含与库目录的时候，也要对应选中相同类型的目标win32，不要选为x64：



1. **为什么我使用strcpy之类标准的c语言函数编译都通不过啊？**

答：涉及到字符串的操作注意新建的工程默认为Unicode字符集，只要函数涉及到字符串操作，一般使用Unicode字符串，要做转换才能使用。如果想按照原来标准的c语言方式使用，可以在项目属性中把字符集改为使用多字节字符集。





1. **课设要求有UI吗？**

答：UI属于课程设计中单个计分点，UI可以用命令行，也可以使用图形化GUI，本课程设计是综合的安全工具开发，不同于算法竞赛、攻防竞赛，目标定位于开发出来的程序需要给用户使用，UI是使用的接口，这是软件设计的一个环节。

Btw：大家可以使用自己习惯的工具，比如：QT，python等，写UI。并且建议将行为分析、截获实时展示都放入该UI。

1. **每类行为都有A W两种，都要实现吗？**

答：作为本课程设计，实现其中一种即可。但要求测试的样例也必须是A。

1. **本课程设计被注入的目标程序可以是第三方的进程吗(不是自己开发的)？**

答：当然可以。本课程设计的最终目的就是想去分析现有的一些进程行为，如果大家开发的程序能够实战，用来分析第三方的进程，说明开发成果更具有兼容性与应用价值，建议给予加分。