

信安导论第五次实验报告

PB19051183 吴承泽

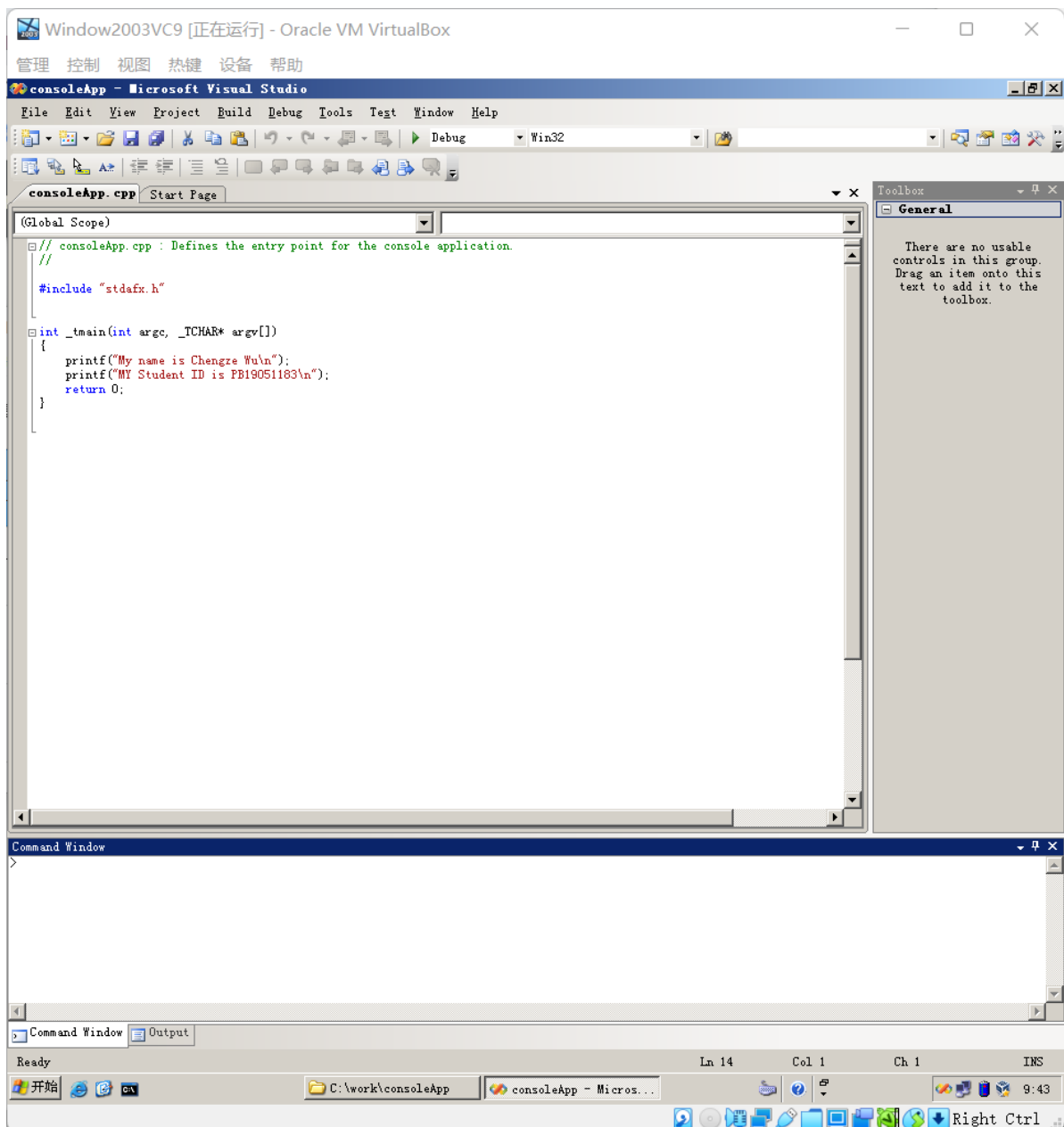
5.3.2 验证PE病毒的步骤

(1) 获得病毒样本

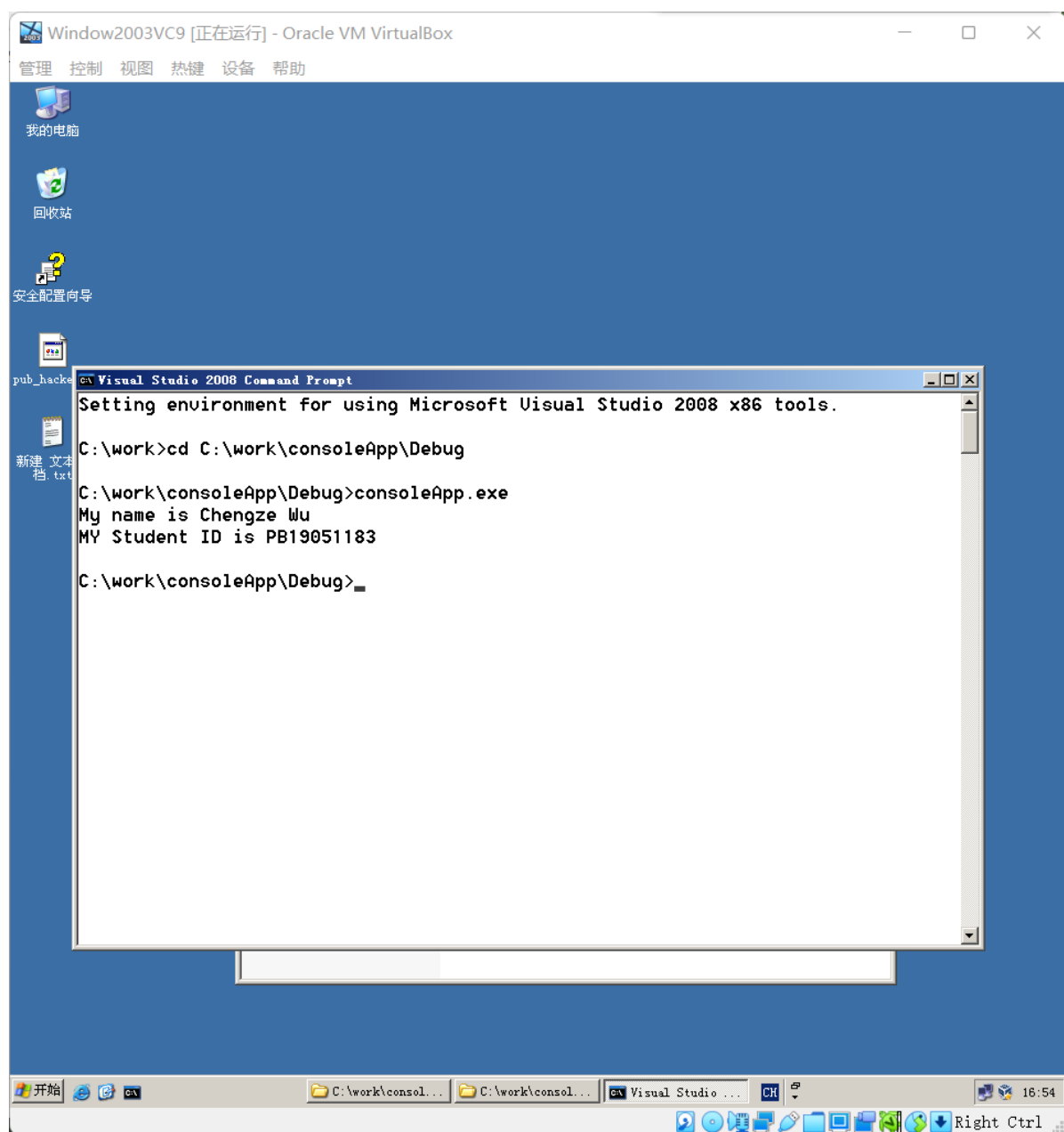
从课程网站下载 AddCode.zip，解压缩到 C:\Work中。

(2) 感染命令程序

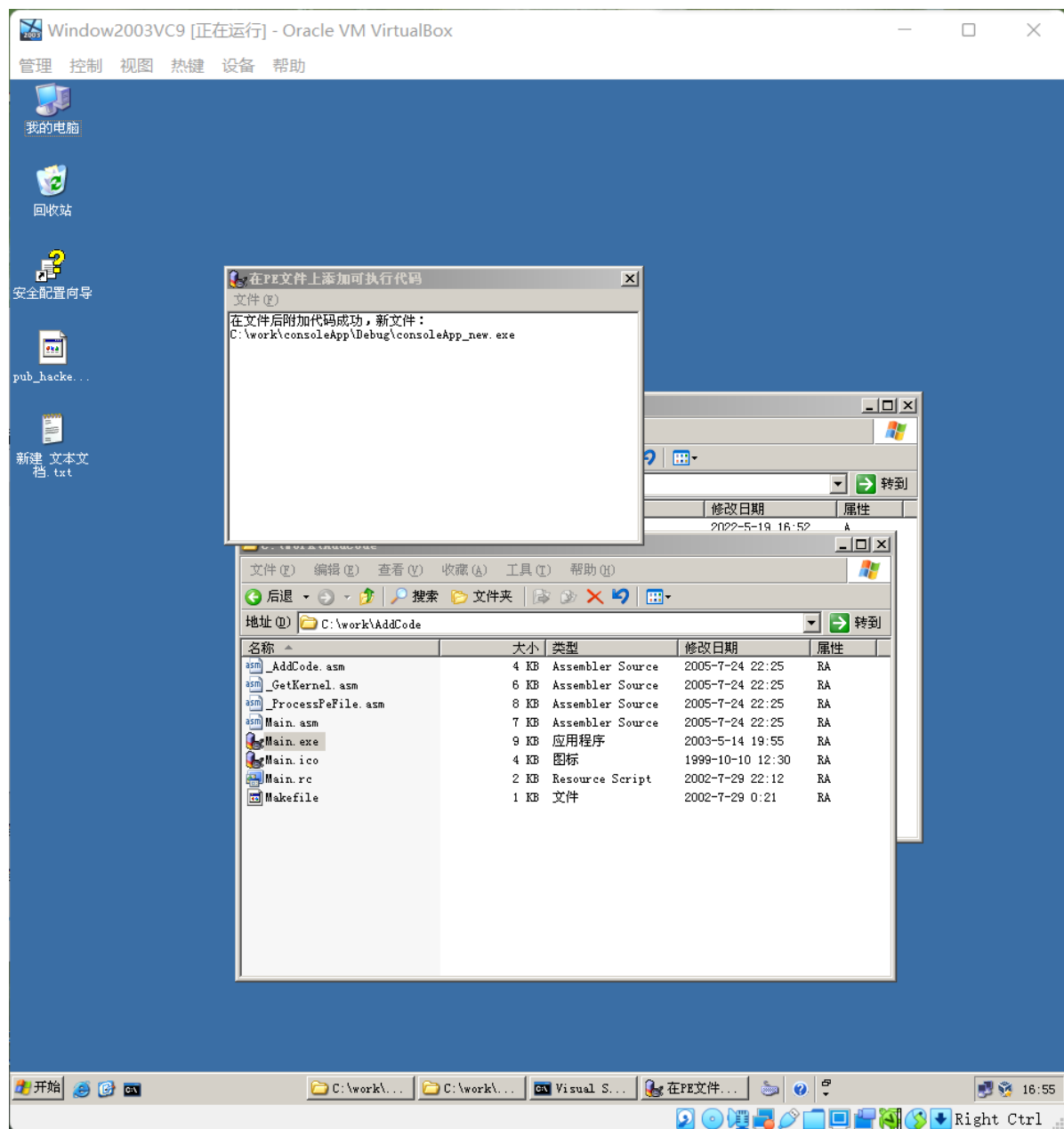
启动 Visual Studio 2008，建立一个 Windows Console 工程，并添加必要的Printf:



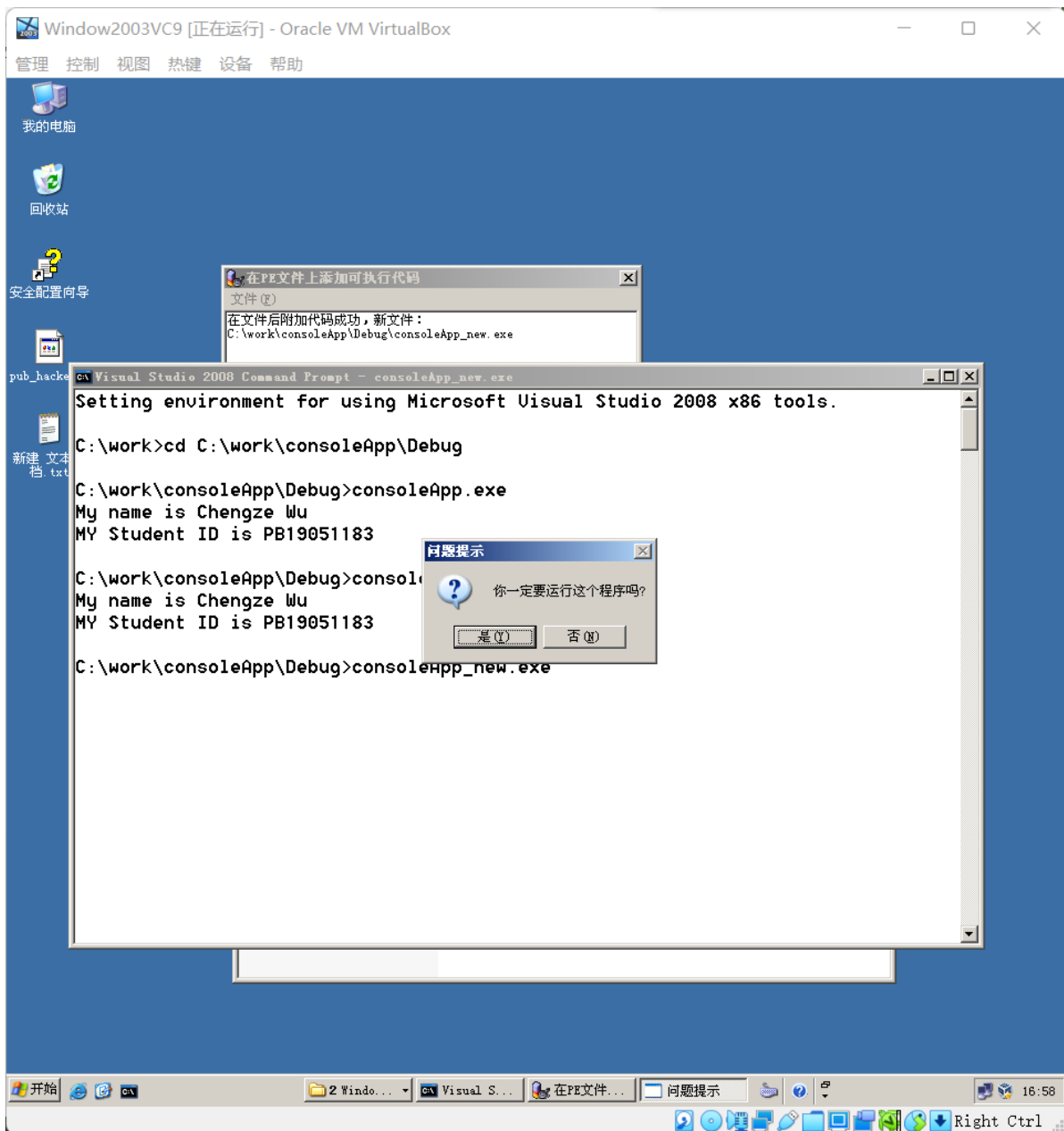
启动命令行，执行未感染的程序：



启动main.exe并感染consoleApp.exe文件后如下：



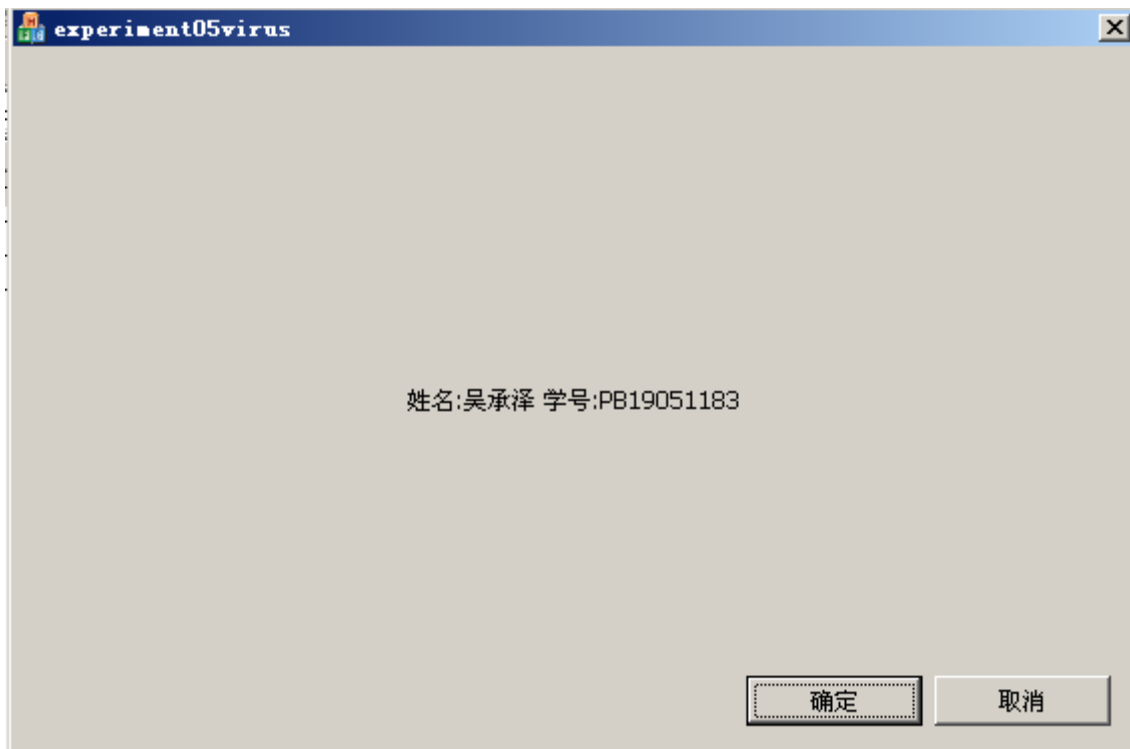
执行感染后的程序consoleApp_nex.exe后，如下所示：



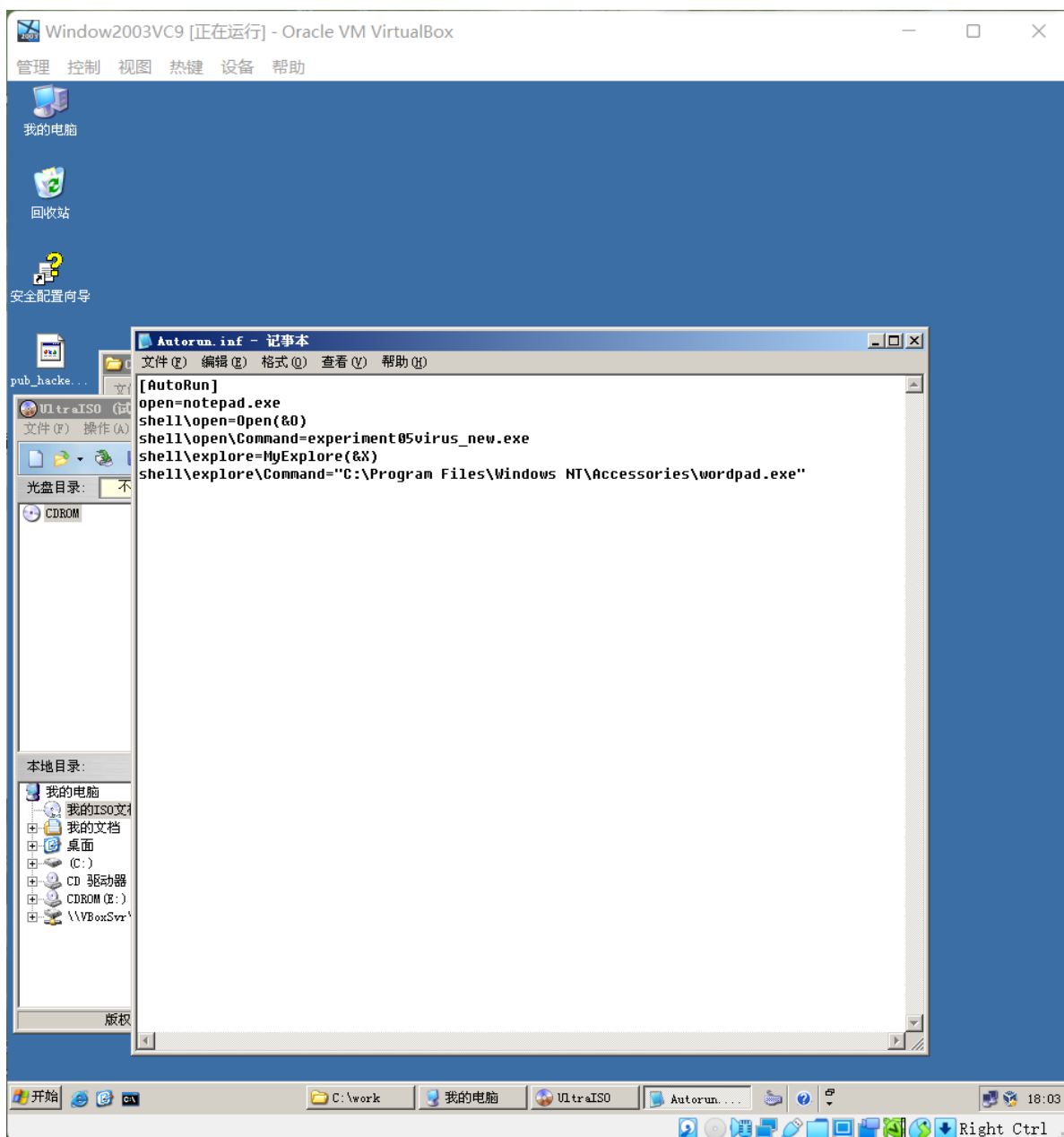
会先弹出一个对话框后，点击确认后执行原来的代码。

5.4

通过Visual Studio 2008设计了一个展示自己学号和姓名的文件如下所示：

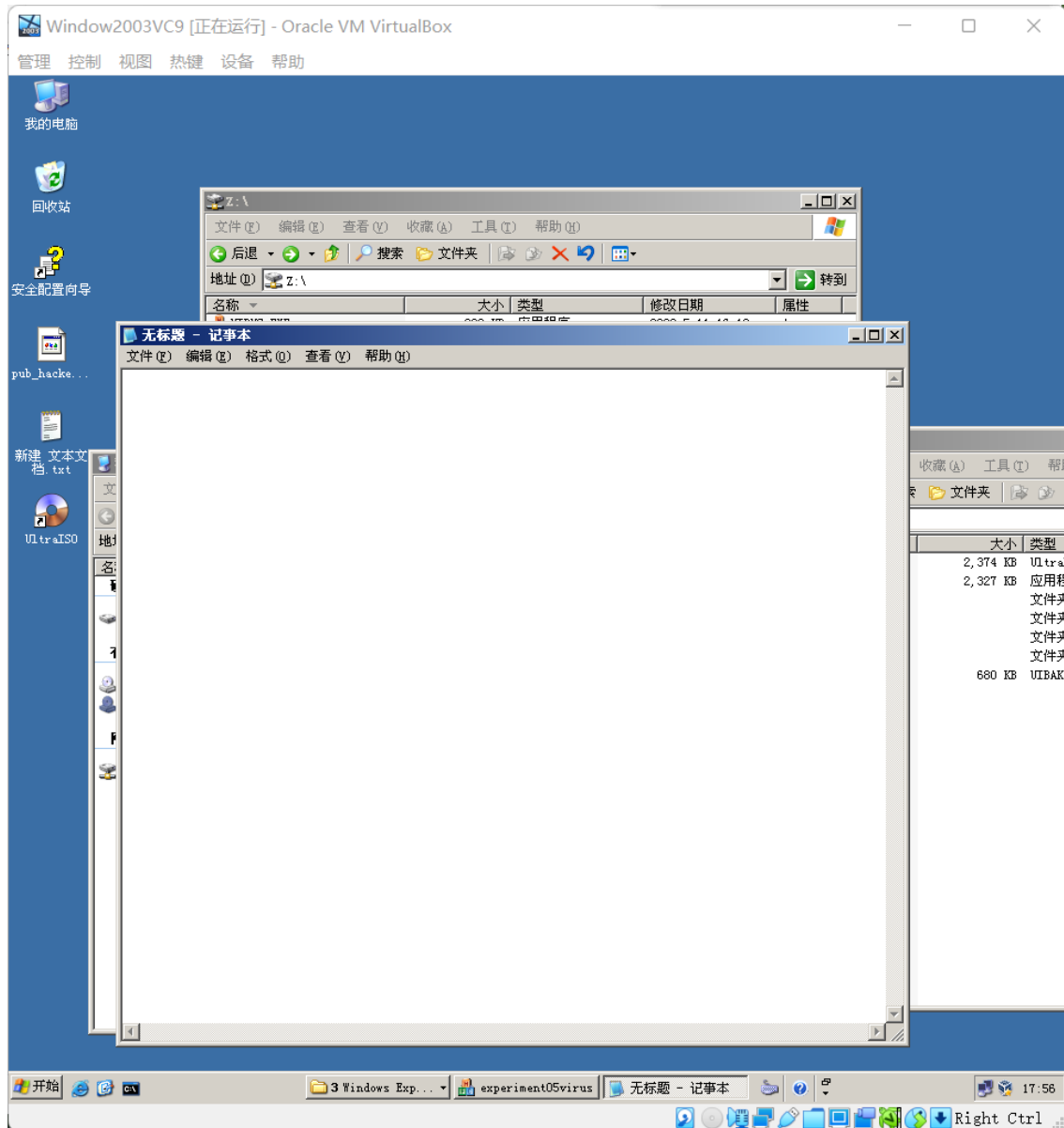


创建自己的光盘映像文件，修改 AUTORUN.INF 文件，命名为 PB19051183.iso。

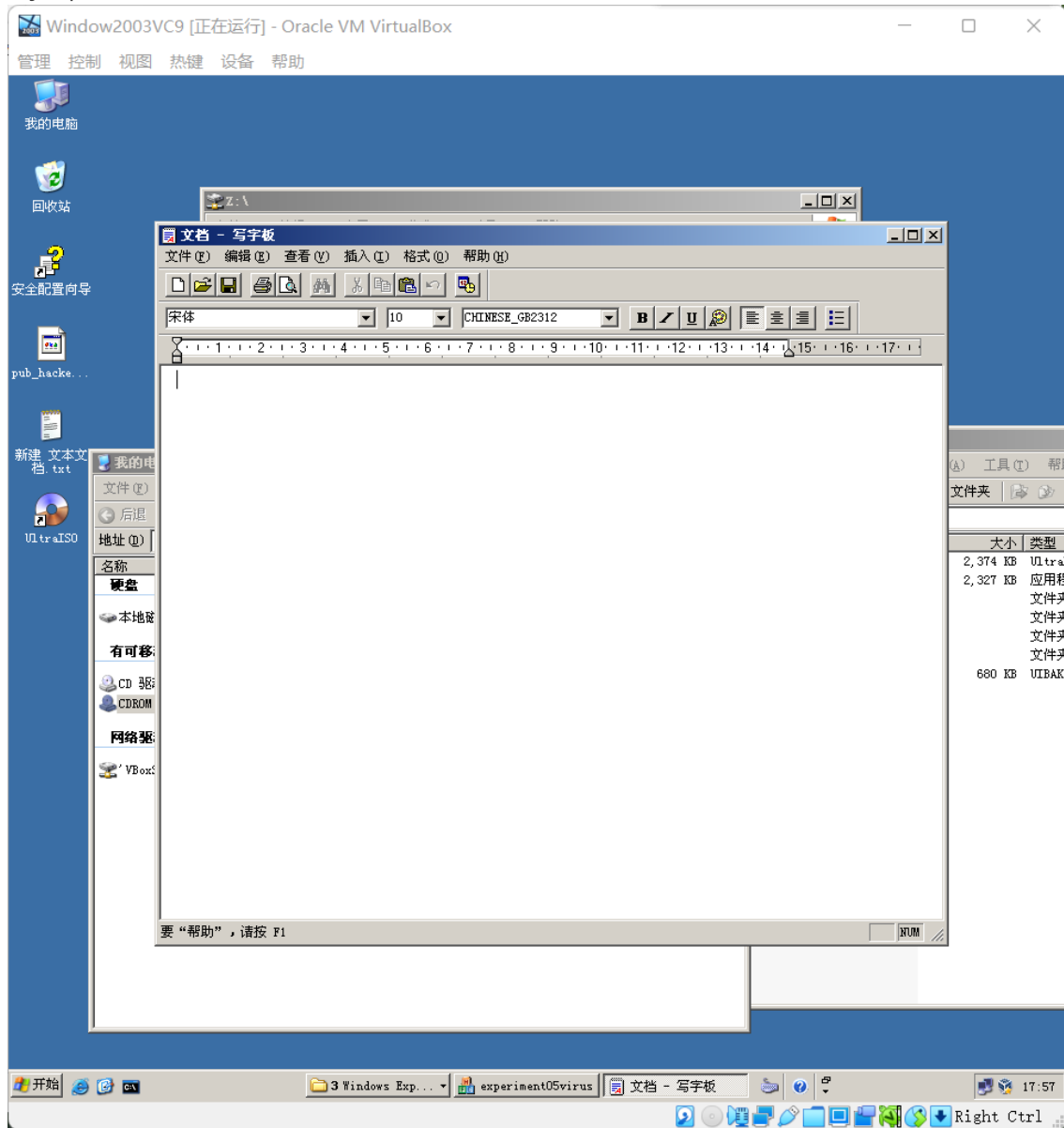


装载后执行如下所示：

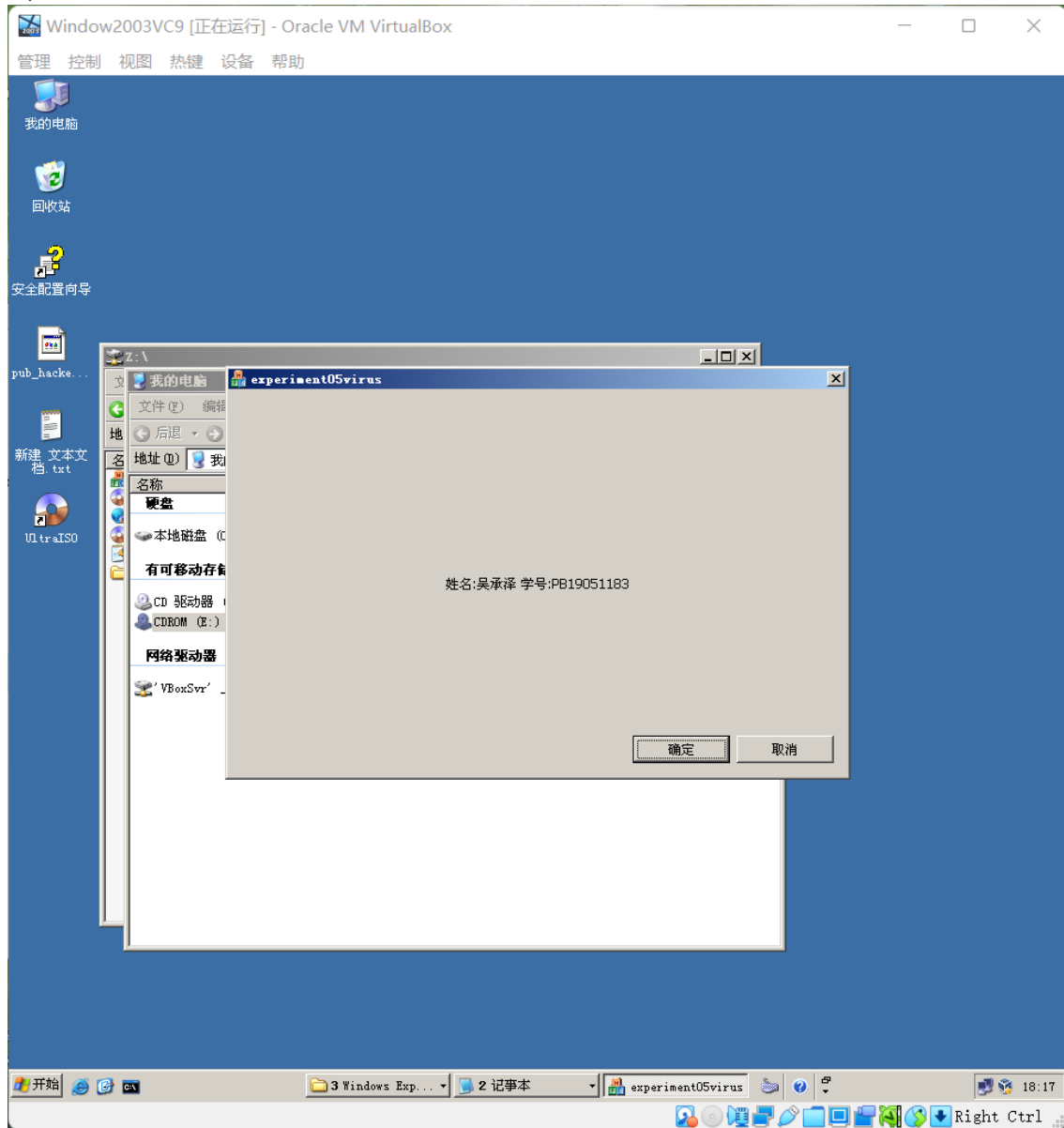
- 自动播放



- MyExplore



- Open



- 双击盘符

