PE病毒实验参考资料：

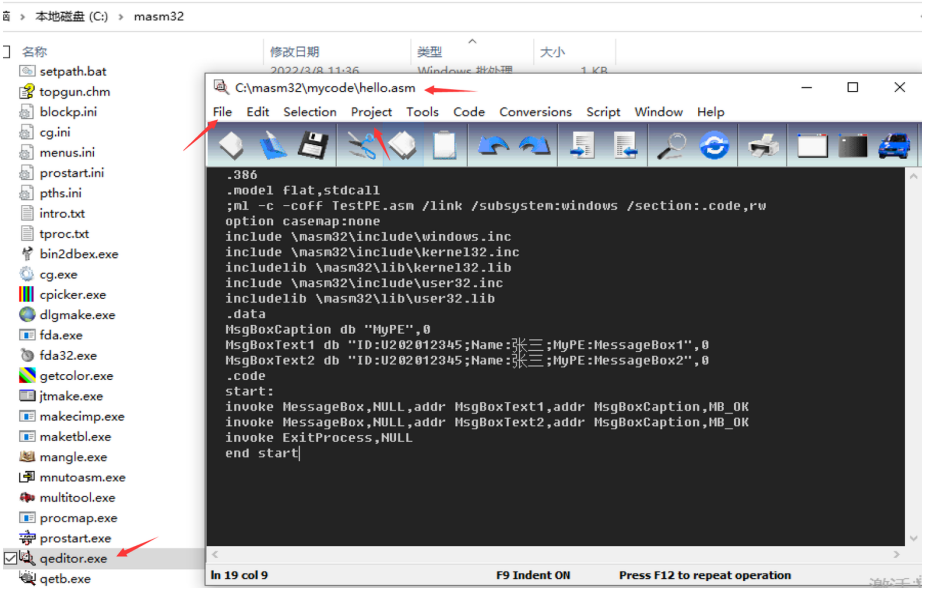
刘铭
华中科技大学

实验注意安全防护，
在虚拟机内进行

环境配置

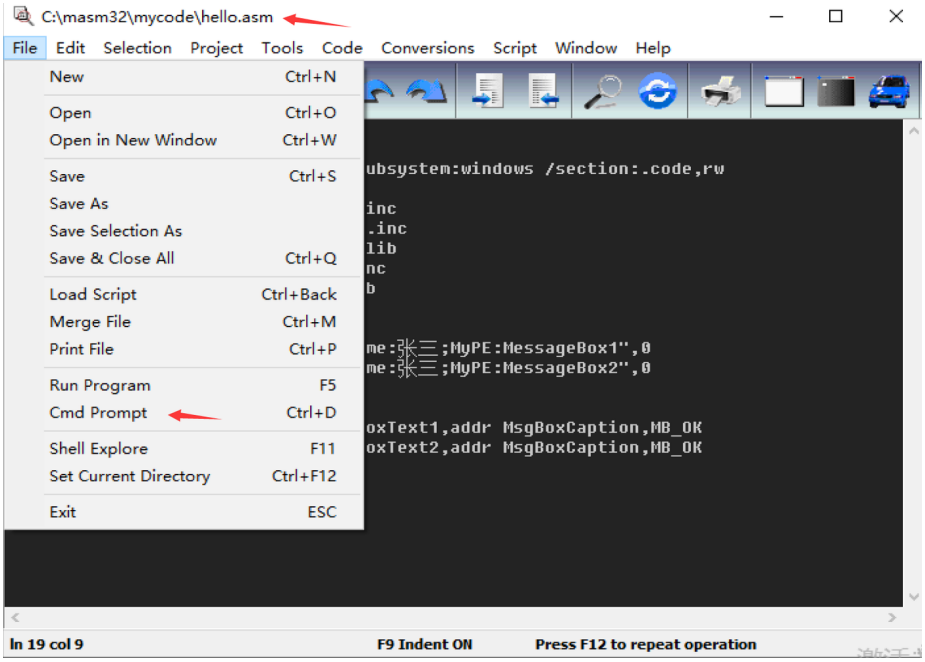
操作系统：win7-32位虚拟机
安全环境：关闭虚拟机的地址随机化等保护措施。
win10:在Windows安全中心中的“应用和浏览器控制”中的“Exploit Protection”中关闭。

软件环境 汇编器、链接器： `masm32 ->qeditor.exe`



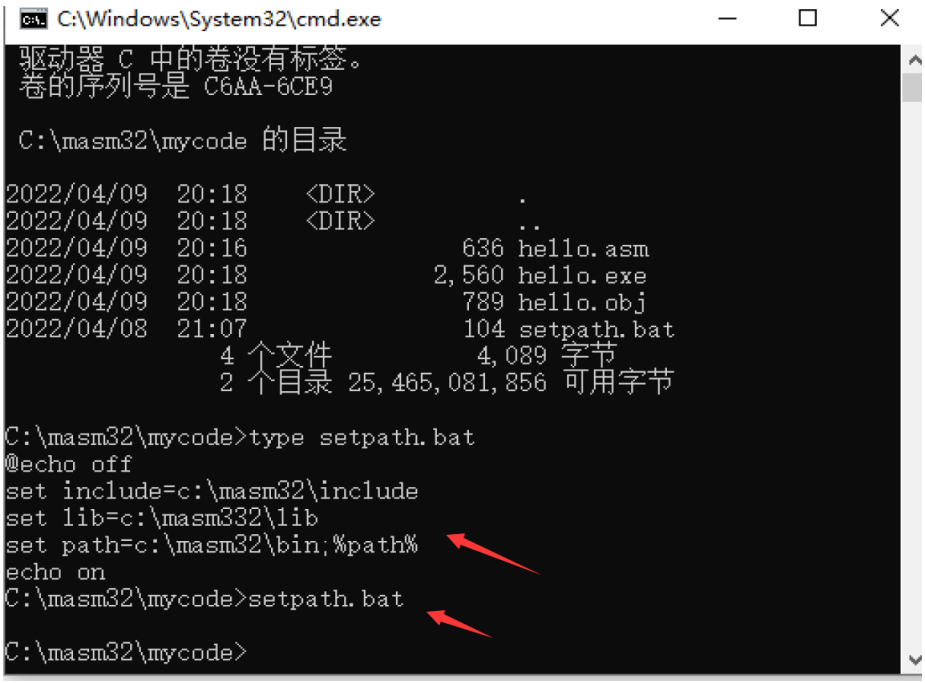
可选环境：vscode和汇编高亮插件 vscode的hex editor

qeditor进入命令行：



环境变量设置的批处理文件： `setpath.bat` 内容及运行

```
@echo off
set include=c:\masm32\include
set lib=c:\masm32\lib
set path=c:\masm32\bin;%path%
echo on
```



命令行：汇编及链接命令参考及运行： `ml /coff /Cp hello.asm /link /subsystem:windows /section:.text,rwe`

链接时，指定生成PE文件**子系统为windows，代码节属性:rwe表示读、写、执行**

```
C:\masm32\mycode>ml /c /coff hello.asm && link /subsystem:windows /section:.text,rwe hello.obj
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: hello.asm

***********
ASCII build
***********

Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.
```

实验探索流程参考

任务1搭建**汇编实验环境。**根据汇编文件MyPE.asm，完成一个在Windows下的**两次**弹窗程序MyPE1.exe，弹窗1显示自己的“学号、姓名、PEHost:MessageBox1”；弹窗2显示“学号、姓名、PEHost:MessageBox2！”

任务2修改PE入口点。手工修改MyPE1.exe二进制文件，修改程序入口点,得到MyPE2.exe，仅运行显示弹窗2;

任务3(重定位，能获得程序运行的基地址与变量预期地址的差，并显示其值。

任务4 获取kernel32.dll的首地址，并存入变量k32Base。

任务5**获取关键函数地址。**通过kernel32.dll导出表查找关键函数在内存中地址并显示。

其他功能 例如**文件搜索**功能：找到当前目录下所有易感染的PE文件；注册表；删除文件；勒索原型；查杀；免杀