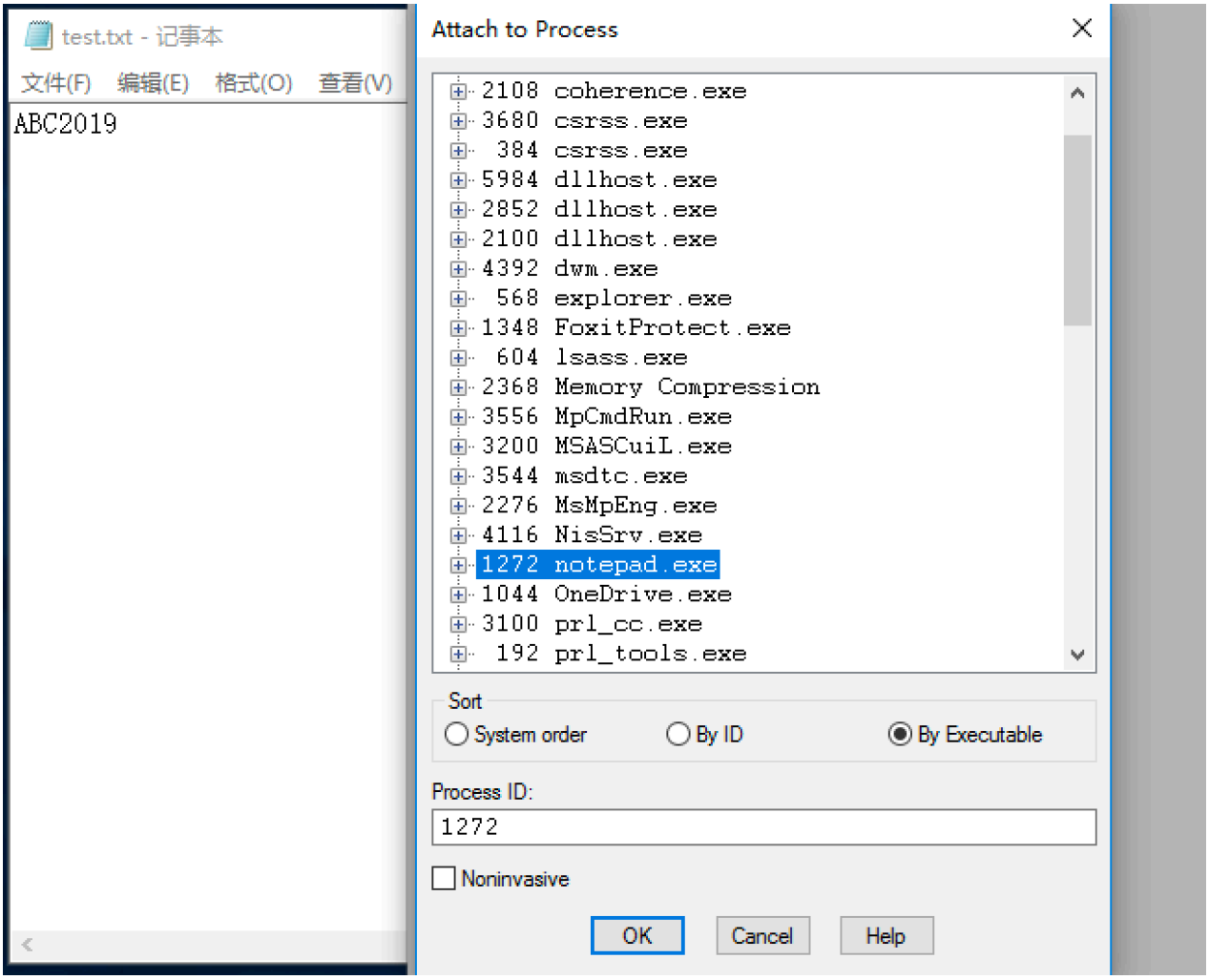
软件与系统安全：任务三

在notepad中，输入一段文字。然后使用调试器，在内存中修改这段文字。使得没有在界面操作notepad的修改文字的情况下。notepad中显示的文字变化。

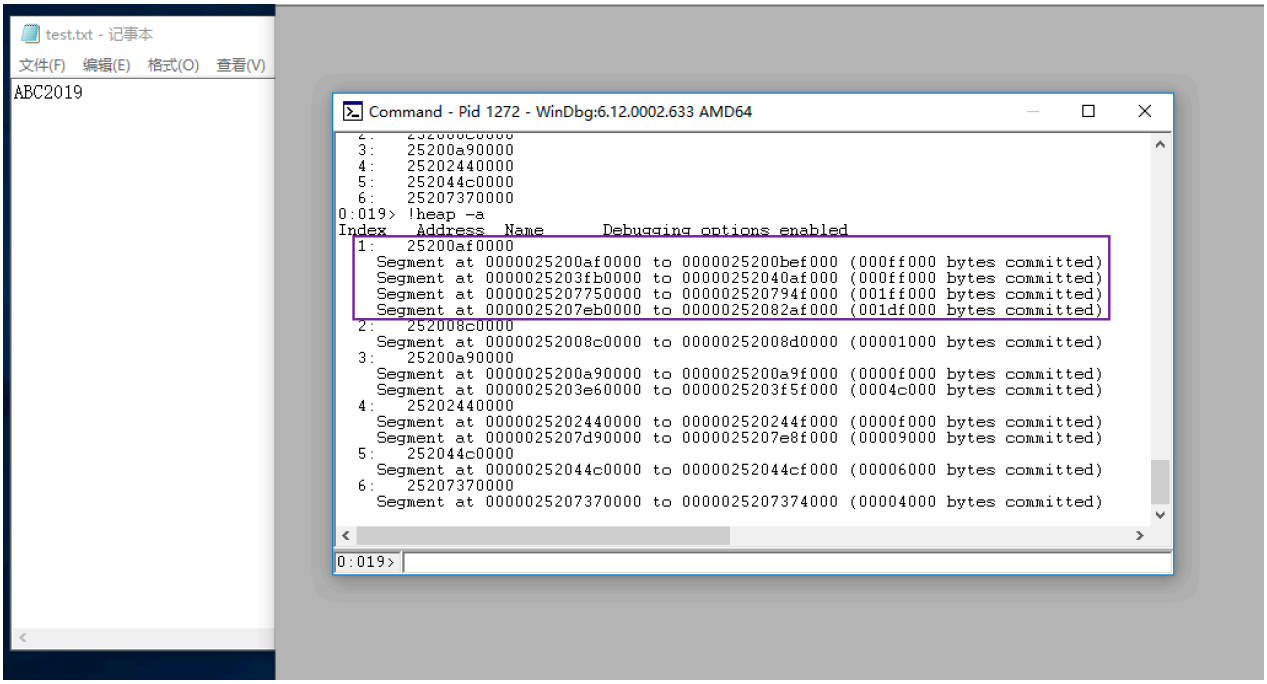
1.首先我们打开notepad并在其中输入文字"ABC2019"，保存文件在固定目录下。打开windbg->attach to a process将其连接到notepad进程。



2.试图列出所有已分配的堆找出字符串"ABC2019"的位置，但是`!heap`指令不识别，由于提示信息可知是部分pdb缺失，因此更改符号表路径并重新载入。

```
0:019> !heap
*******************************************************************************
***                                                                         ***
***                                                                         ***
***    Your debugger is not using the correct symbols                       ***
***                                                                         ***
***    In order for this command to work properly, your symbol path         ***
***    must point to .pdb files that have full type information.            ***
***                                                                         ***
***    Certain .pdb files (such as the public OS symbols) do not            ***
***    contain the required information.  Contact the group that            ***
***    provided you with these symbols if you need this command to          ***
***    work.                                                                ***
***                                                                         ***
***    Type referenced: ntdll!_HEAP_ENTRY                                   ***
***                                                                         ***
*******************************************************************************
Invalid type information
0:019> .reload
Reloading current modules
.....................................................................
.....................................................
```

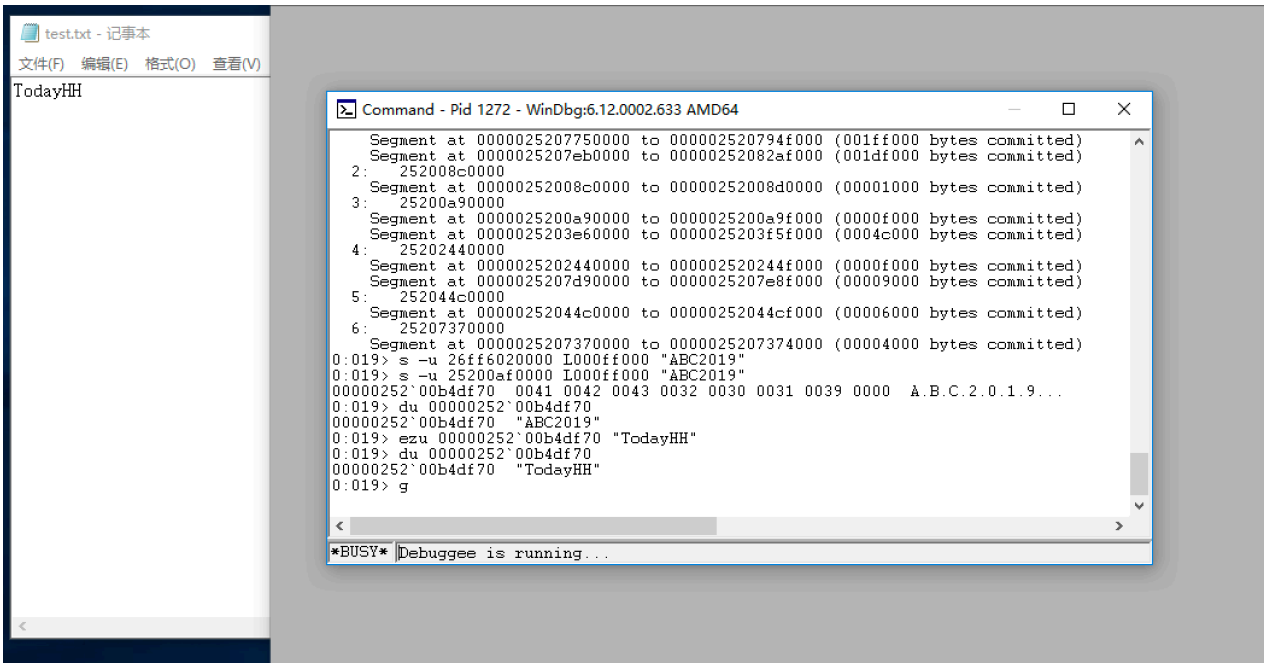
3.更改符号表路径之后该指令`!heap -a`可正确执行，查看后发现有6个已经分配的堆，由于不知道我们所写的字符串在哪个堆中，我们只能一个个尝试



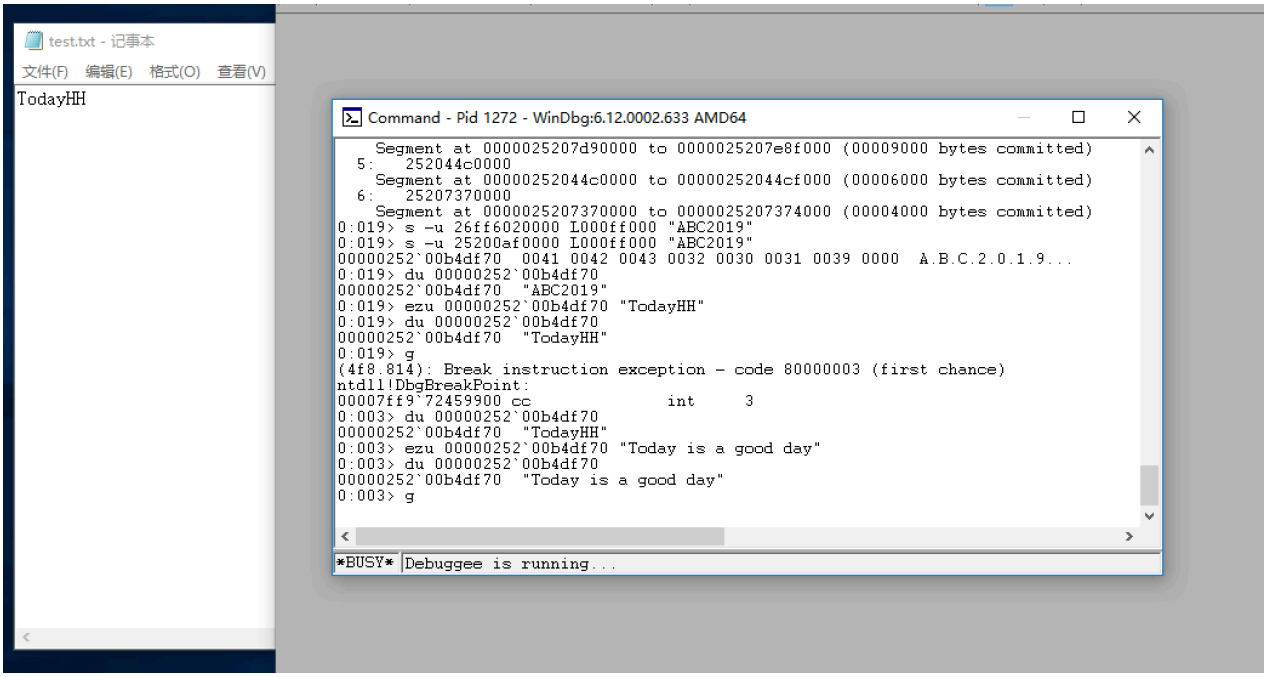
4.从起始位置开始经过固定长度来搜索指定字符串"ABC2019"，查询出一个结果，初步断定这个位置就是我们想要的位置。记录该位置，并用du显示该位置的字符串，确认字符串内容为"ABC2019"

```
0:019> s -u 25200af0000 L000ff000 "ABC2019"
00000252`00b4df70  0041 0042 0043 0032 0030 0031 0039 0000  A.B.C.2.0.1.9...
0:019> du 00000252`00b4df70
00000252`00b4df70  "ABC2019"
```

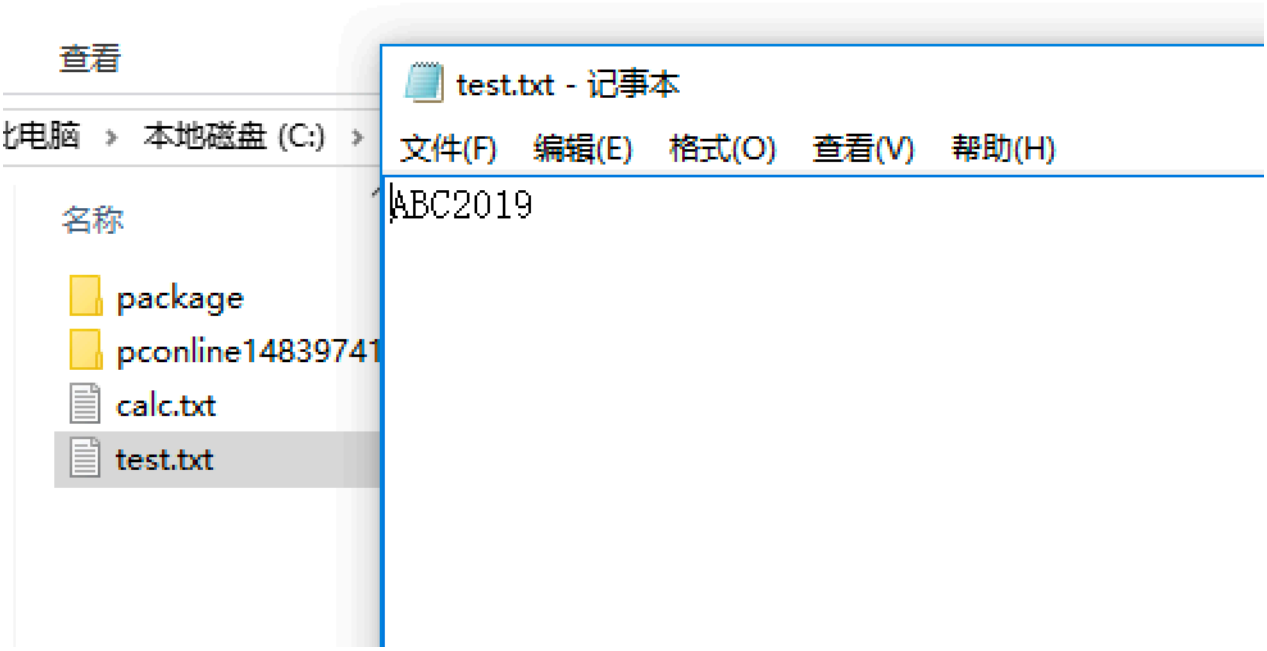
5.对该内存位置的数据进行修改，查看位置字符串，发现内容已经改变，让程序继续运行，发现记事本中显示内容已经变为"TodayHH"



6.发现该办法更改内容字符串的长度只能小于或等于初始字符串长度，如果大于则显示字符串不改变，猜测发生了缓冲区溢出



7.再回头查看保存的txt文件，发现文件内容没有改变，即该方法只是改变了notepad运行过程中的显示字符，没有改变原文件中真实保存的内容


查看
电脑 › 本地磁盘 (C:) ›
名称
package
pconline14839741
calc.txt
test.txt
test.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
ABC2019