一、实验任务

1.编写一个 Realease 版本的 hello world 程序，通过修改程序可执行文件的方式（不是修改源代码），使得程序运行后显示的内容不是 hello world，变成 hello cuc!

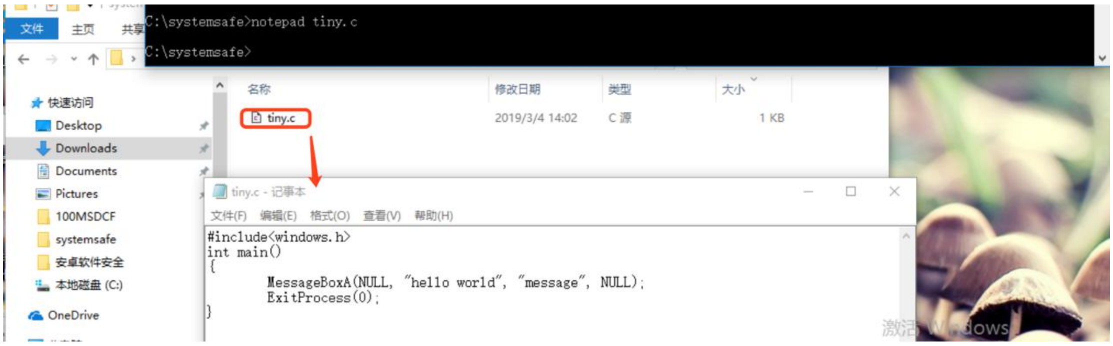
【提示】 一定要在编译选项中将调试信息相关的编译连接选项去掉，否则程序体积会比较大，而且存在很多“干扰”信息。

2.上一题的程序中，修改的显示内容变为一个很长的字符串（至少 2kb 长）。并且保证程序正常运行不崩溃。

【提示】提示，可执行文件中原有的空间有限，必须要新加入数据，加入数据后必须要修改.text 字段中的指针。

二、实验过程

1.1 编写 tiny.c

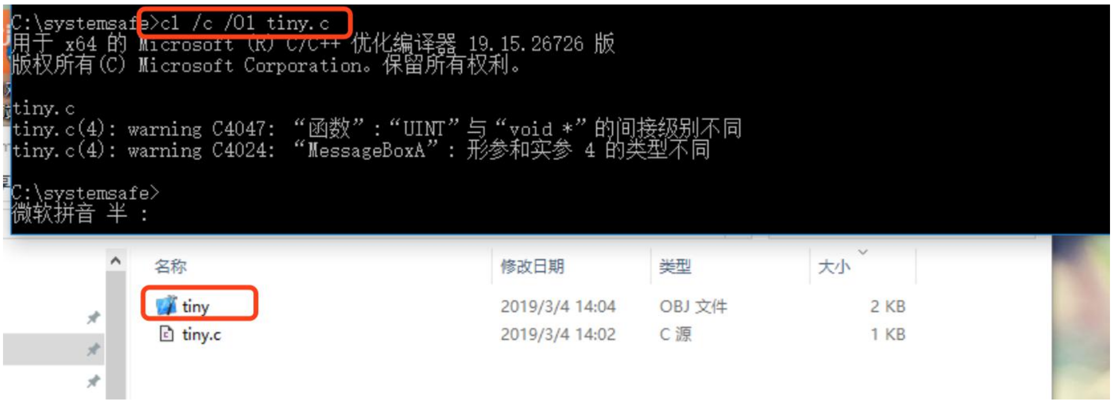


```
C:\systemsafe>notepad tiny.c

C:\systemsafe>
```

```
#include<windows.h>
int main()
{
        MessageBoxA(NULL, "hello world", "message", NULL);
        ExitProcess(0);
}
```

1.2 tiny.c 编译为 tiny.obj

```
cl /c /O1 tiny.c
```

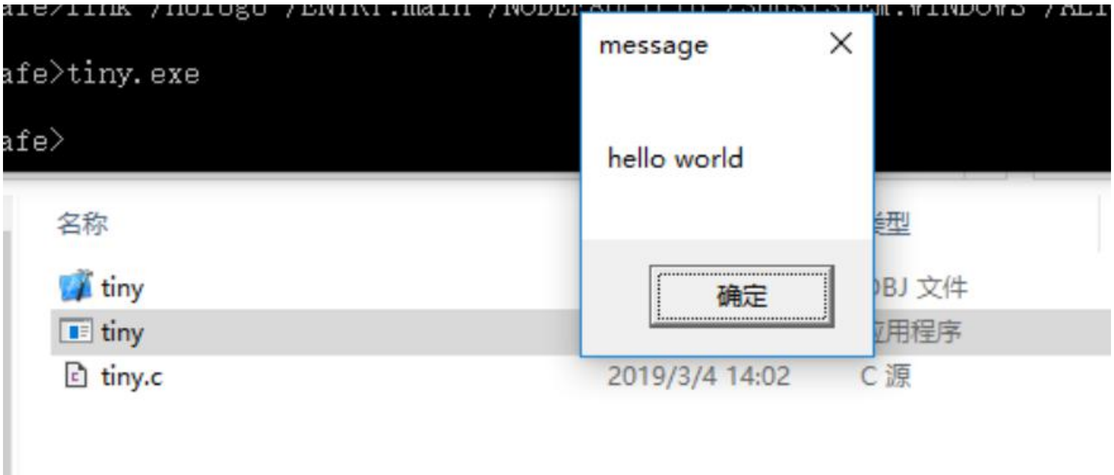


```
C:\systemsafe>cl /c /O1 tiny.c
用于 x64 的 Microsoft (R) C/C++ 优化编译器 19.15.26726 版
版权所有(C) Microsoft Corporation。保留所有权利。

tiny.c
tiny.c(4): warning C4047: “函数”:“UINT”与“void *”的间接级别不同
tiny.c(4): warning C4024: “MessageBoxA”: 形参和实参 4 的类型不同

C:\systemsafe>
微软拼音 半 :
```

名称	修改日期	类型	大小
tiny	2019/3/4 14:04	OBJ 文件	2 KB
tiny.c	2019/3/4 14:02	C 源	1 KB

1.3 tiny.obj 链接为 tiny.exe

```
link /nologo /ENTRY:main /NODEFAULTLIB /SUBSYSTEM:WINDOWS
/ALIGN:16 /DRIVER user32.lib kernel32.lib tiny.obj
```

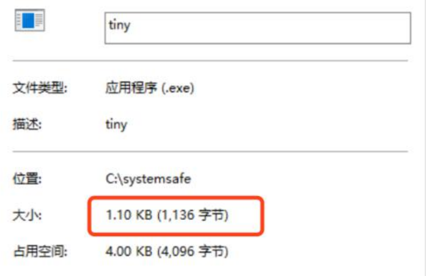


```
afe>link /nologo /ENTRY:main /NODEFAULTLIB /SUBSYSTEM:WINDOWS /ALI

afe>tiny.exe

afe>
```

message

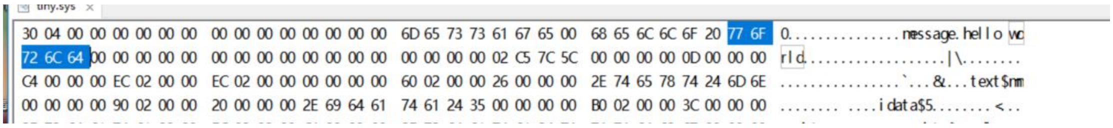
hello world

名称		类型
tiny		OBJ 文件
tiny		应用程序
tiny.c	2019/3/4 14:02	C 源



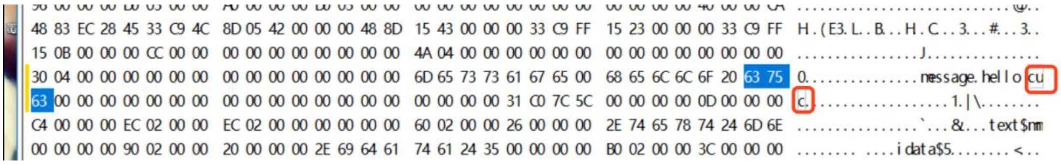
	tiny
文件类型:	应用程序 (.exe)
描述:	tiny
位置:	C:\systemsafe
大小:	1.10 KB (1,136 字节)
占用空间:	4.00 KB (4,096 字节)

1.4 二进制编辑器打开 tiny.exe, 搜索函数 MessageBoxA 显示“hello world”对应 16 进制字段。



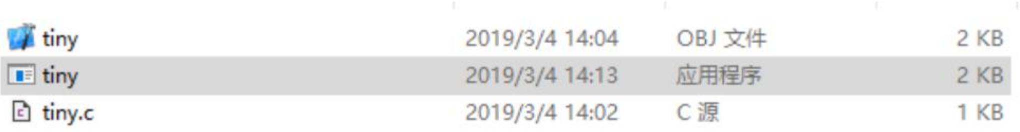
```
30 04 00 00 00 00 00 00  00 00 00 00 00 00 00 00  6D 65 73 73 61 67 65 00  68 65 6C 6C 6F 20 77 6F  0..............message.hello wo
72 6C 64 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 02 C5 7C 5C  00 00 00 00 0D 00 00 00  rld..................|\........
C4 00 00 00 EC 02 00 00  EC 02 00 00 00 00 00 00  60 02 00 00 26 00 00 00  2E 74 65 78 74 24 6D 6E  ................`...&...text$mn
00 00 00 00 90 02 00 00  20 00 00 00 2E 69 64 61  74 61 24 35 00 00 00 00  B0 02 00 00 3C 00 00 00  ........ ....idata$5........<..
```

1.5 修改“world”对应的十六进制值“77 6f 72 6c 64”为，“cuc”对应的十六进制值“63 75 63”，保存并关闭 16 进制编辑器。

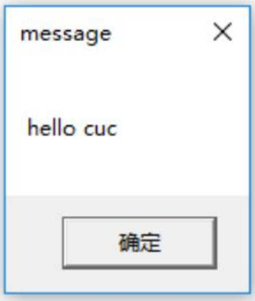


```
48 83 EC 28 45 33 C9 4C  8D 05 42 00 00 00 48 8D  15 43 00 00 00 33 C9 FF  15 23 00 00 00 33 C9 FF  H.(E3.L..B...H.C..3...#...3..
15 0B 00 00 00 CC 00 00  00 00 00 00 00 00 00 00  4A 04 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ...............J...............
30 04 00 00 00 00 00 00  00 00 00 00 00 00 00 00  6D 65 73 73 61 67 65 00  68 65 6C 6C 6F 20 63 75  0..............message.hello cu
63 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 31 C0 7C 5C  00 00 00 00 0D 00 00 00  c.................1.|\.......
C4 00 00 00 EC 02 00 00  EC 02 00 00 00 00 00 00  60 02 00 00 26 00 00 00  2E 74 65 78 74 24 6D 6E  ...............`...&...text$mn
00 00 00 00 90 02 00 00  20 00 00 00 2E 69 64 61  74 61 24 35 00 00 00 00  B0 02 00 00 3C 00 00 00  ........ ....idata$5........<..
```

1.6 运行被修改的 tiny.exe，成功实现通过修改可执行文件使得显示内容从“hello world”变为“hello cuc”。



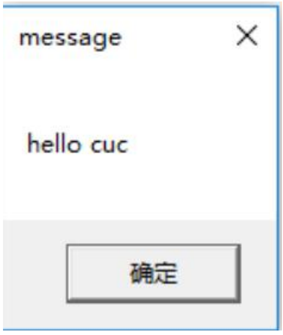
tiny	2019/3/4 14:04	OBJ 文件	2 KB
tiny	2019/3/4 14:13	应用程序	2 KB
tiny.c	2019/3/4 14:02	C 源	1 KB



message

hello cuc

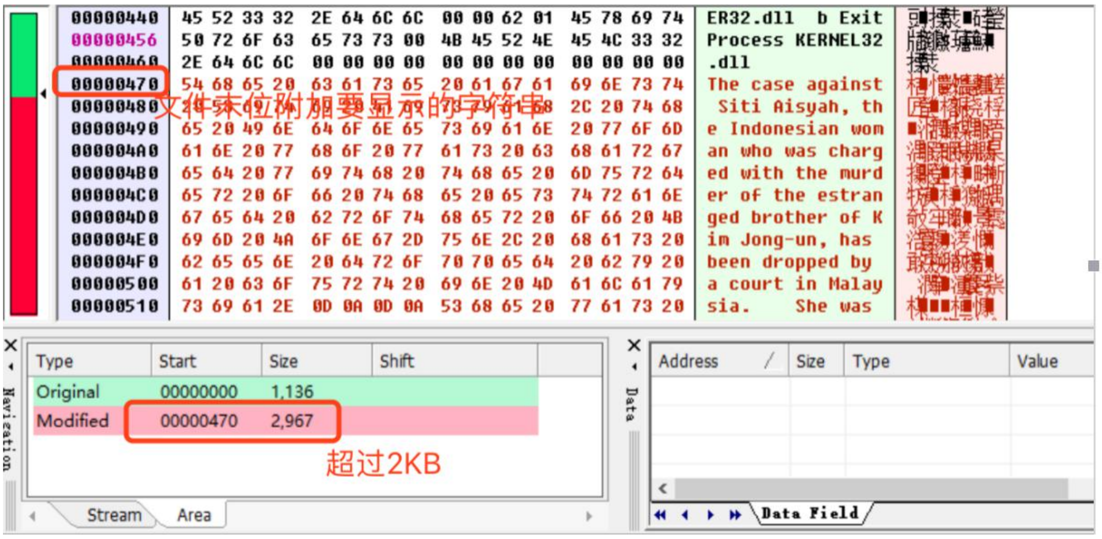
2.1 运行 tiny.exe



message

hello cuc

2.2 用 FlexHEX 以 16 进制打开 tiny.exe，并在文件末位附加要修改显示的超过 2kb 的数据字符串



```
00000440  45 52 33 32  2E 64 6C 6C  00 00 62 01  45 78 69 74  ER32.dll  b Exit
00000456  50 72 6F 63  65 73 73 00  4B 45 52 4E  45 4C 33 32  Process KERNEL32
00000460  2E 64 6C 6C  00 00 00 00  00 00 00 00  00 00 00 00  .dll
00000470  54 68 65 20  63 61 73 65  20 61 67 61  69 6E 73 74  The case against
00000480  20 53 69 74  69 20 41 69  73 79 61 68  2C 20 74 68   Siti Aisyah, th
00000490  65 20 49 6E  64 6F 6E 65  73 69 61 6E  20 77 6F 6D  e Indonesian wom
000004A0  61 6E 20 77  68 6F 20 77  61 73 20 63  68 61 72 67  an who was charg
000004B0  65 64 20 77  69 74 68 20  74 68 65 20  6D 75 72 64  ed with the murd
000004C0  65 72 20 6F  66 20 74 68  65 20 65 73  74 72 61 6E  er of the estran
000004D0  67 65 64 20  62 72 6F 74  68 65 72 20  6F 66 20 4B  ged brother of K
000004E0  69 6D 20 4A  6F 6E 67 2D  75 6E 2C 20  68 61 73 20  im Jong-un, has
000004F0  62 65 65 6E  20 64 72 6F  70 70 65 64  20 62 79 20  been dropped by
00000500  61 20 63 6F  75 72 74 20  69 6E 20 4D  61 6C 61 79  a court in Malay
00000510  73 69 61 2E  0D 0A 0D 0A  53 68 65 20  77 61 73 20  sia.    She was
```

文件末位附加要显示的字符串

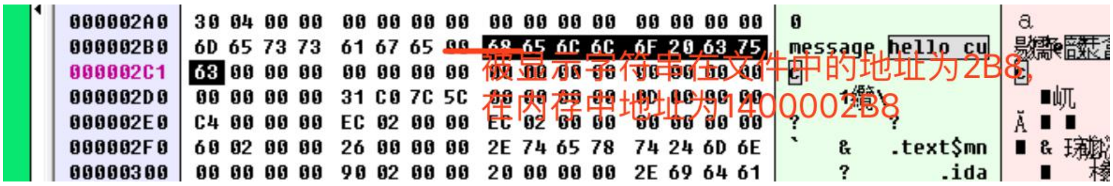
Type	Start	Size	Shift
Original	00000000	1,136	
Modified	00000470	2,967	

超过2KB

2.3 获得 tiny.exe 的反汇编代码,并查看寻找作为参数传入 MessageBoxA 函数的数据字符串在内存中指向其存储地址的指针。

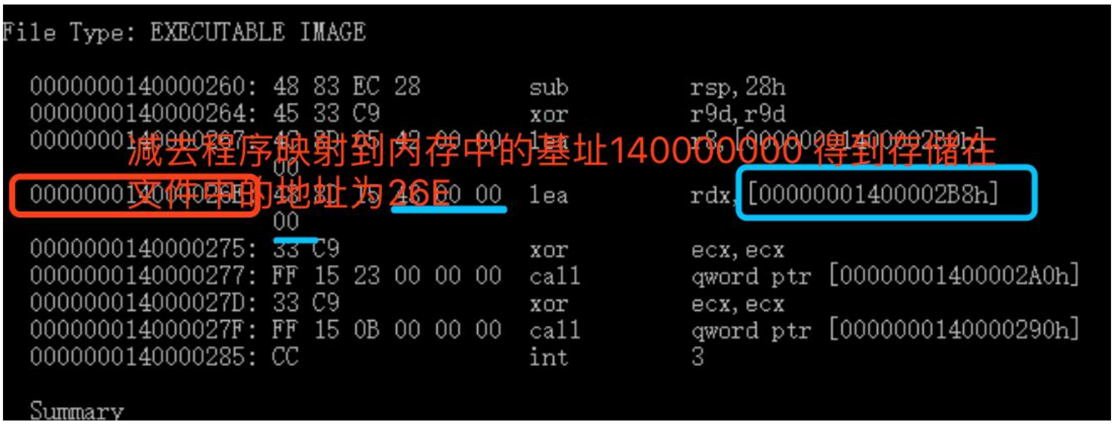
```
Dumpbin /disasm tiny.exe
```

2.4.1 在 16 进制文件查看器 FlexHex 找到存储原被显示字符串“hello cuc”在文件中的存储地址为 2B8h。



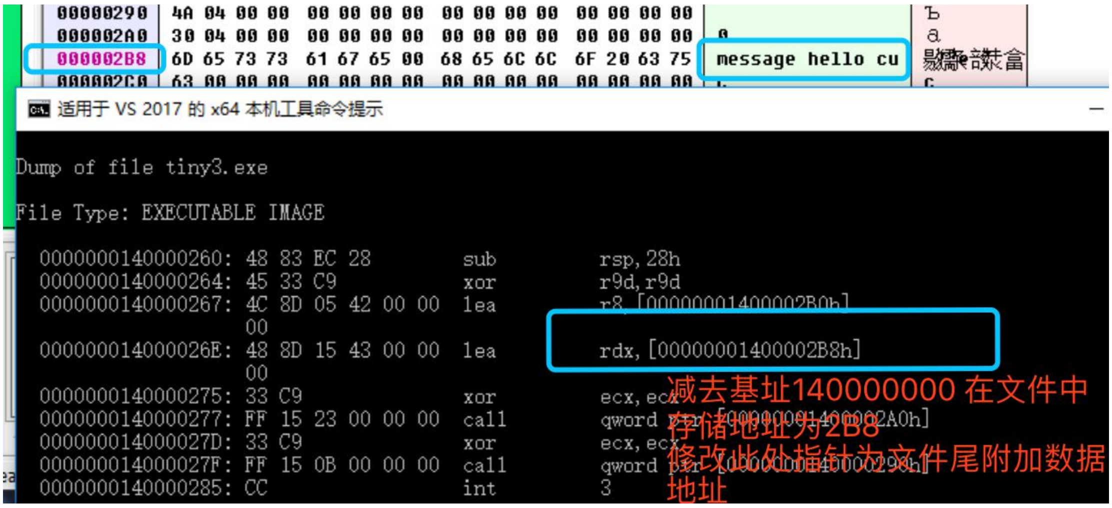
```
000002A0  30 04 00 00  00 00 00 00  00 00 00 00  00 00 00 00  0
000002B0  6D 65 73 73  61 67 65 00  68 65 6C 6C  6F 20 63 75  message hello cu
000002C1  63 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  c
000002D0  00 00 00 00  31 C0 7C 5C  00 00 00 00  0D 00 00 00      1
000002E0  C4 00 00 00  EC 02 00 00  EC 02 00 00  00 00 00 00  ?   ?
000002F0  60 02 00 00  26 00 00 00  2E 74 65 78  74 24 6D 6E  `   &   .text$mn
00000300  00 00 00 00  90 02 00 00  20 00 00 00  2E 69 64 61      ?       .ida
```

被显示字符串在文件中的地址为2B8,
在内存中地址为1400002B8



```
File Type: EXECUTABLE IMAGE

  0000000140000260: 48 83 EC 28           sub         rsp,28h
  0000000140000264: 45 33 C9              xor         r9d,r9d
  0000000140000267: 4C 8D 05 42 00 00     lea         r8,[00000001400002B0h]
                    00
  000000014000026E: 48 8D 15 43 00 00     lea         rdx,[00000001400002B8h]
                    00
  0000000140000275: 33 C9                 xor         ecx,ecx
  0000000140000277: FF 15 23 00 00 00     call        qword ptr [00000001400002A0h]
  000000014000027D: 33 C9                 xor         ecx,ecx
  000000014000027F: FF 15 0B 00 00 00     call        qword ptr [0000000140000290h]
  0000000140000285: CC                    int         3

  Summary
```

减去程序映射到内存中的基址140000000 得到存储在文件中的地址为26E



```
00000290  4A 04 00 00  00 00 00 00  00 00 00 00  00 00 00 00
000002A0  30 04 00 00  00 00 00 00  00 00 00 00  00 00 00 00
000002B8  6D 65 73 73  61 67 65 00  68 65 6C 6C  6F 20 63 75   message hello cu
```

适用于 VS 2017 的 x64 本机工具命令提示

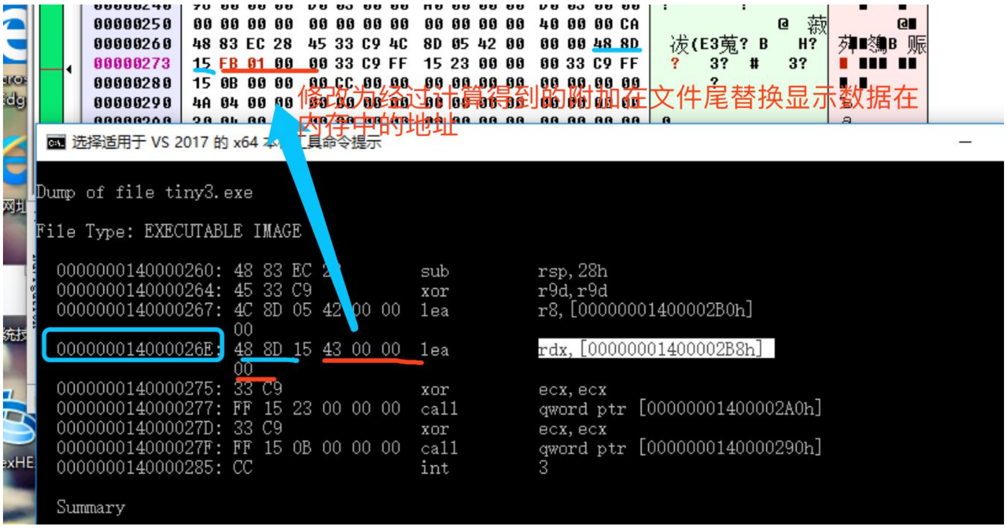
```
Dump of file tiny3.exe

File Type: EXECUTABLE IMAGE

  0000000140000260: 48 83 EC 28         sub         rsp,28h
  0000000140000264: 45 33 C9            xor         r9d,r9d
  0000000140000267: 4C 8D 05 42 00 00   lea         r8,[00000001400002B0h]
                    00
  000000014000026E: 48 8D 15 43 00 00   lea         rdx,[00000001400002B8h]
                    00
  0000000140000275: 33 C9               xor         ecx,ecx
  0000000140000277: FF 15 23 00 00 00   call        qword ptr [00000001400002A0h]
  000000014000027D: 33 C9               xor         ecx,ecx
  000000014000027F: FF 15 0B 00 00 00   call        qword ptr [0000000140000290h]
  0000000140000285: CC                  int         3
```

减去基址140000000 在文件中存储地址为2B8

修改此处指针为文件尾附加数据地址

2.4.2 在 tiny.exe 的反汇编代码里找到对字符串地址进行操作的语句(即将字符串“hello cuc”作为参数传递给函数 MessageBox 的汇编指令在文件中的存储地址），计算得到该程序命令语句在文件中的存储地址为 26Eh;在 16 进制文件查看器 FlexHex 中定位文件地址 26Eh 处，修改相应 16 进制命令中地址为经过计算后得到的文件末位附加的将被显示的数据字符串的地址 EB 01。

01EBh=43h[原汇编命令语句中指向原字符串“hello cuc”在文件中存储位置的指针]+(470h[目标数据字符串在文件中的存储地址]-2B8h[源字符串“hello cuc”在文件中的存储地址])

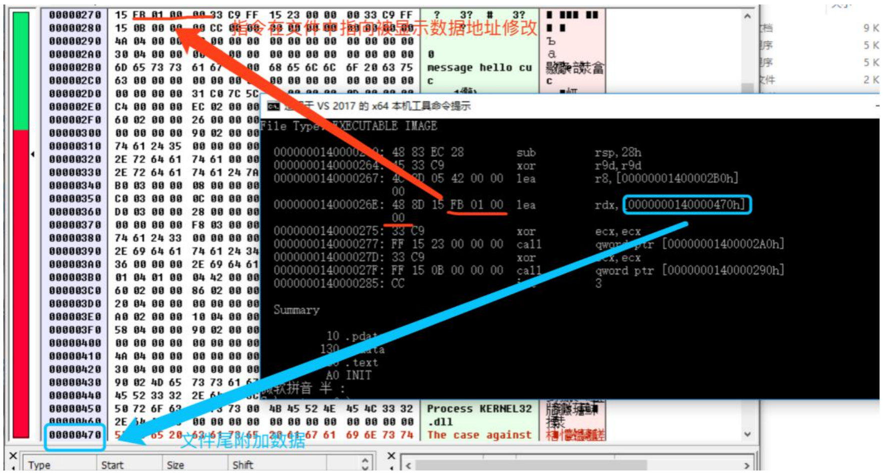


```
00000250  00 00 00 00  00 00 00 00  00 00 00 00  40 00 00 CA
00000260  48 83 EC 28  45 33 C9 4C  8D 05 42 00  00 00 48 8D
00000273  15 EB 01 00  00 33 C9 FF  15 23 00 00  00 33 C9 FF
00000280  15 0B 00 00  00 CC 00 00  00 00 00 00  00 00 00 00
00000290  4A 04 00 00
```

修改为经过计算得到的附加在文件尾替换显示数据在内存中的地址

选择适用于 VS 2017 的 x64 本机工具命令提示

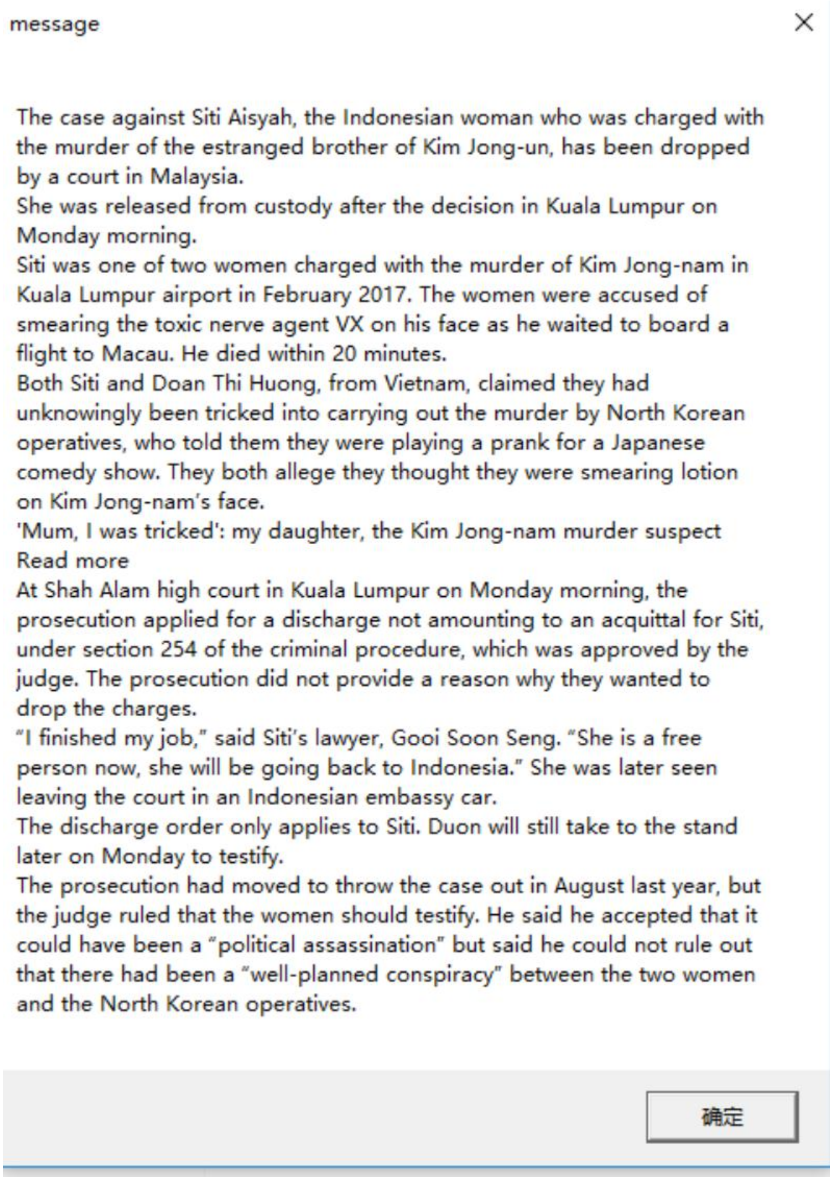
```
Dump of file tiny3.exe

File Type: EXECUTABLE IMAGE

  0000000140000260: 48 83 EC 28         sub         rsp,28h
  0000000140000264: 45 33 C9            xor         r9d,r9d
  0000000140000267: 4C 8D 05 42 00 00   lea         r8,[00000001400002B0h]
                    00
  000000014000026E: 48 8D 15 43 00 00   lea         rdx,[00000001400002B8h]
                    00
  0000000140000275: 33 C9               xor         ecx,ecx
  0000000140000277: FF 15 23 00 00 00   call        qword ptr [00000001400002A0h]
  000000014000027D: 33 C9               xor         ecx,ecx
  000000014000027F: FF 15 0B 00 00 00   call        qword ptr [0000000140000290h]
  0000000140000285: CC                  int         3

  Summary
```



指令在文件中指向被显示数据地址修改
文件尾附加数据
VS 2017 的 x64 本机工具命令提示

```
File Type: EXECUTABLE IMAGE

  0000000140000260: 48 83 EC 28          sub         rsp,28h
  0000000140000264: 45 33 C9             xor         r9d,r9d
  0000000140000267: 4C 8D 05 42 00 00    lea         r8,[00000001400002B0h]
                    00
  000000014000026E: 48 8D 15 FB 01 00    lea         rdx,[0000000140000470h]
                    00
  0000000140000275: 33 C9                xor         ecx,ecx
  0000000140000277: FF 15 23 00 00 00    call        qword ptr [00000001400002A0h]
  000000014000027D: 33 C9                xor         ecx,ecx
  000000014000027F: FF 15 0B 00 00 00    call        qword ptr [0000000140000290h]
  0000000140000285: CC                   int         3

  Summary

          10 .pdata
         130 .rdata
          10 .text
          A0 INIT
```

2.5 关闭保存修改后的文件, 再次运行 tiny.exe,成功显示添加在文件尾的大于 2kb 长的字符串



message

The case against Siti Aisyah, the Indonesian woman who was charged with the murder of the estranged brother of Kim Jong-un, has been dropped by a court in Malaysia.
She was released from custody after the decision in Kuala Lumpur on Monday morning.
Siti was one of two women charged with the murder of Kim Jong-nam in Kuala Lumpur airport in February 2017. The women were accused of smearing the toxic nerve agent VX on his face as he waited to board a flight to Macau. He died within 20 minutes.
Both Siti and Doan Thi Huong, from Vietnam, claimed they had unknowingly been tricked into carrying out the murder by North Korean operatives, who told them they were playing a prank for a Japanese comedy show. They both allege they thought they were smearing lotion on Kim Jong-nam's face.
'Mum, I was tricked': my daughter, the Kim Jong-nam murder suspect
Read more
At Shah Alam high court in Kuala Lumpur on Monday morning, the prosecution applied for a discharge not amounting to an acquittal for Siti, under section 254 of the criminal procedure, which was approved by the judge. The prosecution did not provide a reason why they wanted to drop the charges.
"I finished my job," said Siti's lawyer, Gooi Soon Seng. "She is a free person now, she will be going back to Indonesia." She was later seen leaving the court in an Indonesian embassy car.
The discharge order only applies to Siti. Duon will still take to the stand later on Monday to testify.
The prosecution had moved to throw the case out in August last year, but the judge ruled that the women should testify. He said he accepted that it could have been a "political assassination" but said he could not rule out that there had been a "well-planned conspiracy" between the two women and the North Korean operatives.

三、实验问题

1.在进行第二个任务中，已经发现指向原字符串“hello cuc”在文件中存储地址的指针为00000001400002B8h，不知道如何通过修改16进制字符内容，修改命令中指针的指向。

解决：

1.1 计算文件中地址为26Eh处指令指向地址

2B8h=1400002B8h-140000000h(程序映射到内存中的基址)

01EBh=43h[原汇编命令语句中指向原字符串“hello cuc”在文件中存储位置的指针]+(470h[目标数据字符串在文件中的存储地址]-2B8h[源字符串“hello cuc”在文件中的存储地址])

1.2 修改43 00 00 00为EB 01 00 00