

题1-2实验报告

程序源码

```
#include <stdio.h>
#include <windows.h>

int main()
{
    MessageBoxA(NULL, "hello world!", "hello world!", MB_OK);
    ExitProcess(0);
}
```

1、编写一个release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为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。

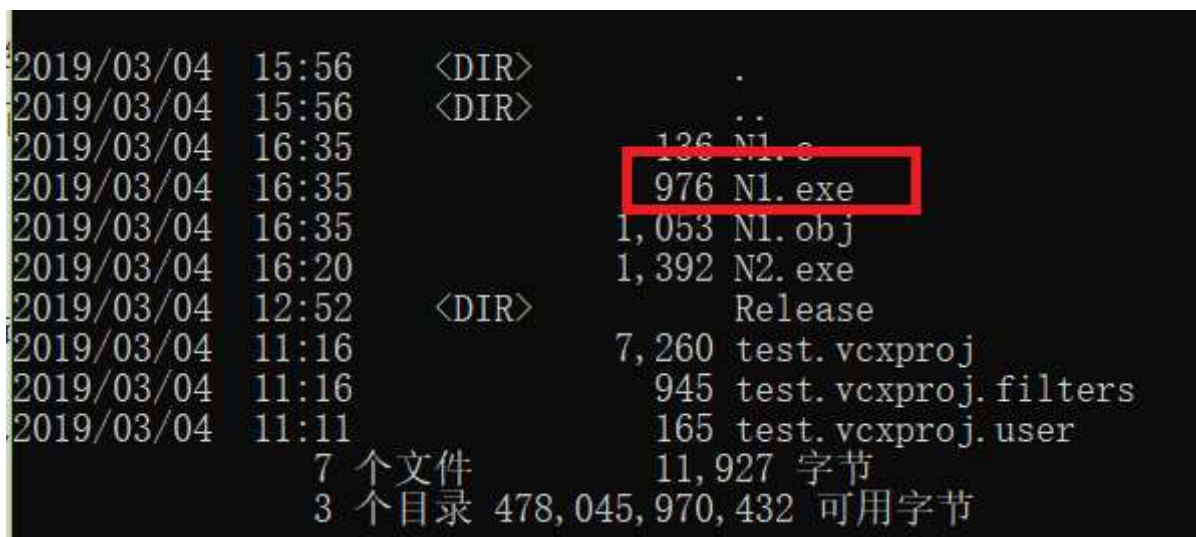
实验步骤

- 减少生成的可执行文件的体积

```
cl /c /O1 N1.c
```

```
# 修改入口,只链接需要的库,减小文件对齐
```

```
link /ENTRY:main /NODEFAULTLIB User32.lib kernel32.lib /ALIGN:16 N1.obj
```



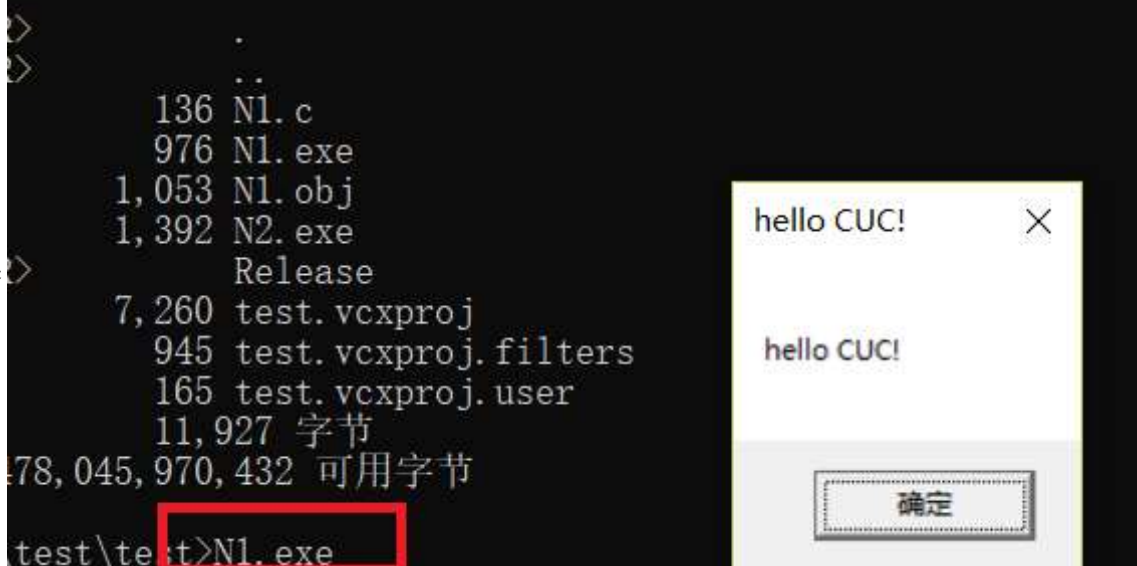
```
2019/03/04 15:56 <DIR> .
2019/03/04 15:56 <DIR> ..
2019/03/04 16:35 136 N1.c
2019/03/04 16:35 976 N1.exe
2019/03/04 16:35 1,053 N1.obj
2019/03/04 16:20 1,392 N2.exe
2019/03/04 12:52 <DIR> Release
2019/03/04 11:16 7,260 test.vcxproj
2019/03/04 11:16 945 test.vcxproj.filters
2019/03/04 11:11 165 test.vcxproj.user
7 个文件 11,927 字节
3 个目录 478,045,970,432 可用字节
```

- 使用winhex修改字符串 hello world 为 hello cuc!

00000230	6A 00 B8 60 02 40 00 50	50 6A 00 FF 15 58 02 40	j , ' @ PPj y X @
00000240	00 6A 00 FF 15 50 02 40	00 CC 00 00 00 00 00 00	j y P @ i
00000250	96 03 00 00 00 00 00 00	7C 03 00 00 00 00 00 00	-
00000260	58 65 6C 6C 6F 20 77 6F	72 6C 64 21 00 00 00 00	hello world!
00000270	00 00 00 00 59 E3 7C 5C	00 00 00 00 0D 00 00 00	Yä \
00000280	A4 00 00 00 8C 02 00 00	8C 02 00 00 00 00 00 00	× E E
00000290	30 02 00 00 1A 00 00 00	2E 74 65 78 74 24 6D 6E	0 .text\$mn
000002A0	00 00 00 00 50 02 00 00	10 00 00 00 2E 69 64 61	P .ida
000002B0	74 61 24 35 00 00 00 00	60 02 00 00 2C 00 00 00	ta\$5 ,
000002C0	2E 72 64 61 74 61 00 00	8C 02 00 00 A4 00 00 00	.rdata E ×
000002D0	2E 72 64 61 74 61 24 7A	7A 7A 64 62 67 00 00 00	.rdata\$zzzdbg

00000230	6A 00 B8 60 02 40 00 50	50 6A 00 FF 15 58 02 40	j , ' @ PPj y X @
00000240	00 6A 00 FF 15 50 02 40	00 CC 00 00 00 00 00 00	j y P @ i
00000250	96 03 00 00 00 00 00 00	7C 03 00 00 00 00 00 00	-
00000260	68 65 6C 6C 6F 20 43 55	43 21 00 00 00 00 00 00	hello CUC!
00000270	00 00 00 00 59 E3 7C 5C	00 00 00 00 0D 00 00 00	Yä \
00000280	A4 00 00 00 8C 02 00 00	8C 02 00 00 00 00 00 00	× E E
00000290	30 02 00 00 1A 00 00 00	2E 74 65 78 74 24 6D 6E	0 .text\$mn
000002A0	00 00 00 00 50 02 00 00	10 00 00 00 2E 69 64 61	P .ida
000002B0	74 61 24 35 00 00 00 00	60 02 00 00 2C 00 00 00	ta\$5 ,
000002C0	2E 72 64 61 74 61 00 00	8C 02 00 00 A4 00 00 00	.rdata E ×
000002D0	2E 72 64 61 74 61 24 7A	7A 7A 64 62 67 00 00 00	.rdata\$zzzdbg

- 结果



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，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。

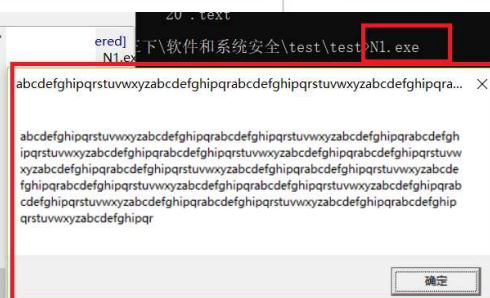
- ```
SECTION HEADER #1
.text name
1A virtual size
230 virtual address (00400230 to 00400249)
20 size of raw data
230 file pointer to raw data (00000230 to 0000024F)
0 file pointer to relocation table
0 file pointer to line numbers
0 number of relocations
0 number of line numbers
60000020 flags
Code
Execute Read

RAW DATA #1
00400230: 6A 00 B8 60 02 40 00 50 50 6A 00 FF 15 58 02 40 j. . . @. PPj. Ÿ. X. @
00400240: 00 6A 00 FF 15 50 02 40 00 CC . j. Ÿ. P. @. I
```

- | offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 0  | A  | B  | C  | D  | E  | F  | ANSI ASCII | Code         |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------|--------------|
| 00000000 | 50 | 02 | 00 | 00 | 00 | 40 | 00 | 10 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | P          | 0            |
| 00000010 | 06 | 00 | 00 | 00 | 00 | 00 | 00 | 06 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | N1.exe     | Execute Read |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | EAT        |              |
| 00000030 | 00 | 03 | 00 | 00 | 30 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 03 | 04 | 85 | B  | 0  | 0          |              |
| 00000040 | 00 | 00 | 10 | 00 | 00 | 10 | 00 | 00 | 00 | 10 | 00 | 00 | 10 | 00 | 00 | 00 | 00 | 0          | <            |
| 00000050 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 50 | 02 | 00 | 10 | 00 | 00 | 00 | 00 | 00 | 00 | P          |              |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 2E | 74 | 65 | 78 | 74 | 24 | 6D | 6E | 0  | 0  |            |              |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000200 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000210 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000220 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0          |              |
| 00000230 | 00 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |            |              |



| Offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F                |                | ANSI ASCII |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|----------------|------------|
| 000001C0 | 1A | 00 | 00 | 00 | 30 | 02 | 00 | 00 | 20 | 00 | 00 | 00 | 30 | 02 | 00 | 00               | 0              | 0          |
| 000001D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 | 00 | 60               |                |            |
| 000001E0 | 2E | 72 | 64 | 61 | 74 | 61 | 00 | 00 | 62 | 01 | 00 | 00 | 50 | 02 | 00 | 00               | .rdata b P     |            |
| 000001F0 | 70 | 01 | 00 | 00 | 50 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00               | P P            |            |
| 00000200 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 40 | 2E | 72 | 65 | 6C | 6F | 63 | 00 | 00               | @ @.relac      |            |
| 00000210 | 10 | 00 | 00 | 00 | C0 | 03 | 00 | 00 | 10 | 00 | 00 | 00 | C0 | 03 | 00 | 00               | À À            |            |
| 00000220 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 42               | @ B            |            |
| 00000230 | 6A | 00 | B8 | 00 | 03 | 40 | 50 | 50 | 5A | 00 | FF | 15 | 58 | 02 | 40 | j ,d @ PPj y X @ |                |            |
| 00000240 | 00 | 6A | 00 | FF | 15 | 50 | 02 | 40 | 00 | CC | 00 | 00 | 00 | 00 | 00 | 00               | j y p @ i      |            |
| 00000250 | 96 | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 7C | 03 | 00 | 00 | 00 | 00 | 00 | 00               | -              |            |
| 00000260 | 68 | 65 | 6C | 6C | 6F | 20 | 43 | 53 | 45 | 21 | 00 | 00 | 00 | 00 | 00 | 00               | hello CUC!     |            |
| 00000270 | 00 | 00 | 00 | 00 | 8A | 00 | 00 | 00 | 8C | 00 | 00 | 00 | 00 | 00 | 00 | 00               | Yà\            |            |
| 00000280 | A4 | 00 | 00 | 00 | 8C | 02 | 00 | 00 | 8C | 02 | 00 | 00 | 00 | 00 | 00 | 00               | = @ E          |            |
| 00000290 | 30 | 02 | 00 | 00 | 1A | 00 | 00 | 00 | 2E | 74 | 65 | 78 | 74 | 24 | 6D | 6E               | 0 .text\$mn    |            |
| 000002A0 | 00 | 00 | 00 | 00 | 50 | 02 | 00 | 00 | 10 | 00 | 00 | 00 | 2E | 69 | 64 | 61               | P .ida         |            |
| 000002B0 | 74 | 61 | 24 | 35 | 00 | 00 | 00 | 00 | 60 | 02 | 00 | 00 | 2C | 00 | 00 | 00               | ta\$5          |            |
| 000002C0 | 2E | 72 | 64 | 61 | 74 | 61 | 00 | 00 | 8C | 02 | 00 | 00 | A4 | 00 | 00 | 00               | .rdata E =     |            |
| 000002D0 | 2E | 72 | 64 | 61 | 74 | 61 | 24 | 7A | 7A | 7A | 64 | 62 | 67 | 00 | 00 | 00               | .rdata\$zzzdbg |            |
| 000002E0 | 30 | 03 | 00 | 00 | 28 | 00 | 00 | 00 | 2E | 69 | 64 | 61 | 74 | 61 | 24 | 32               | 0 (.ida\$2     |            |
| 000002F0 | 00 | 00 | 00 | 00 | 5B | 03 | 00 | 00 | 14 | 00 | 00 | 00 | 2E | 69 | 64 | 61               | X .ida         |            |
| 00000300 | 74 | 61 | 24 | 33 | 00 | 00 | 00 | 00 | 6C | 03 | 00 | 00 | 10 | 00 | 00 | 00               | ta\$3 l        |            |
| 00000310 | 2E | 69 | 64 | 61 | 74 | 61 | 24 | 34 | 00 | 00 | 00 | 00 | 7C | 03 | 00 | 00               | .ida\$4        |            |
| 00000320 | 36 | 00 | 00 | 00 | 2E | 69 | 64 | 61 | 74 | 61 | 24 | 36 | 00 | 00 | 00 | 00               | 6 .ida\$6      |            |
| 00000330 | 74 | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 8A | 03 | 00 | 00               | t \$           |            |
| 00000340 | 58 | 02 | 00 | 00 | 6C | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00               | X l            |            |
| 00000350 | A4 | 03 | 00 | 00 | 50 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00               | = P            |            |
| 00000360 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 96 | 03 | 00 | 00               | -              |            |
| 00000370 | 00 | 00 | 00 | 00 | 7C | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 89 | 02 | 4D               | 65             |            |
| 00000380 | 73 | 73 | 61 | 67 | 65 | 42 | 6F | 58 | 01 | 45 |    |    |    |    |    |                  |                |            |

 $32 = 2E2$ [illegible]

Icons

catch

c@ffsle

=Bytes

No2c

1999b].

3. **fractal**

Temp