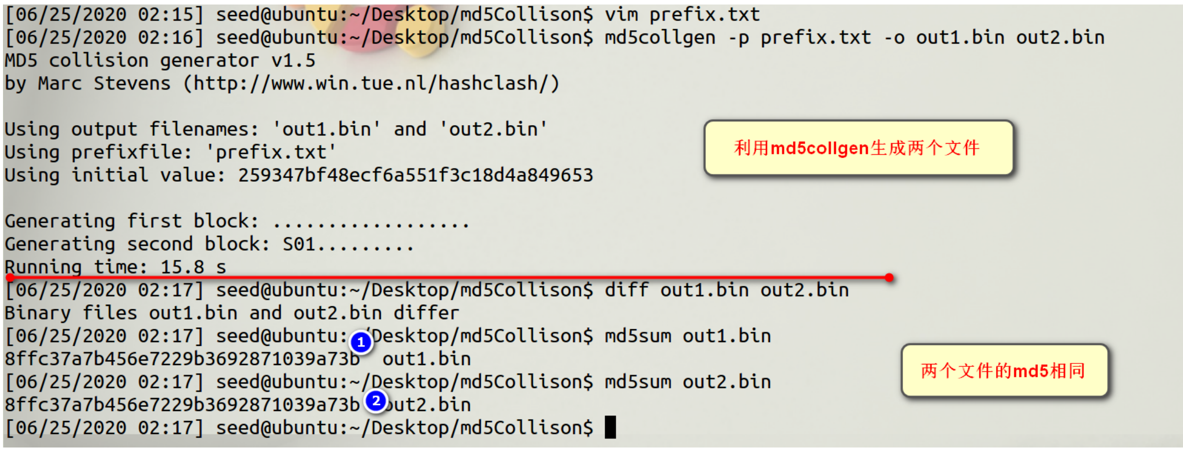
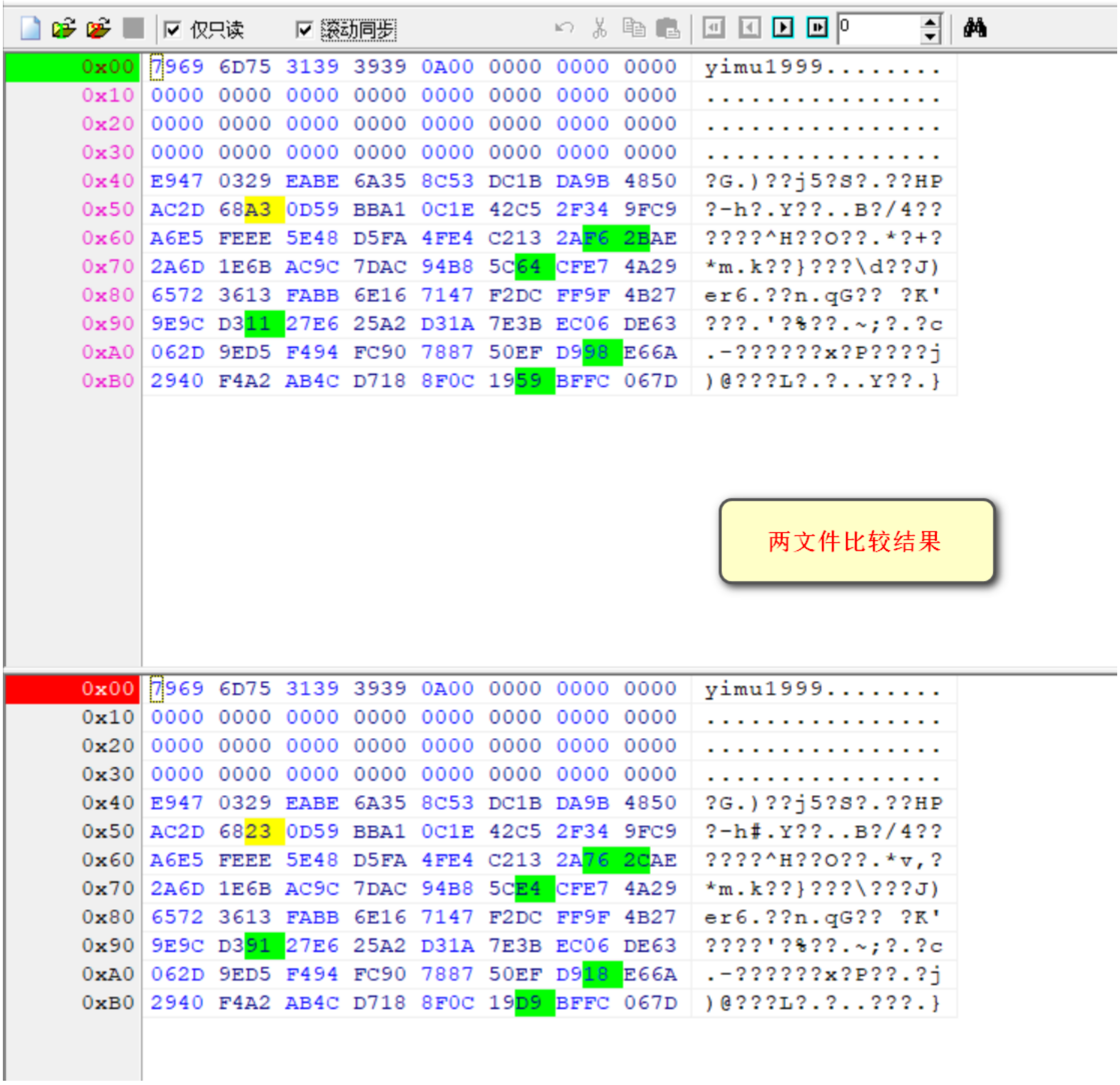
2020 Spring MD5 Collision Attack Lab

Task 1: Generating Two Different Files with the Same MD5 Hash



```
[06/25/2020 02:15] seed@ubuntu:~/Desktop/md5Collison$ vim prefix.txt
[06/25/2020 02:16] seed@ubuntu:~/Desktop/md5Collison$ md5collgen -p prefix.txt -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: 259347bf48ecf6a551f3c18d4a849653

Generating first block: .................
Generating second block: S01.........
Running time: 15.8 s
[06/25/2020 02:17] seed@ubuntu:~/Desktop/md5Collison$ diff out1.bin out2.bin
Binary files out1.bin and out2.bin differ
[06/25/2020 02:17] seed@ubuntu:~/Desktop/md5Collison$ md5sum out1.bin
8ffc37a7b456e7229b3692871039a73b  out1.bin
[06/25/2020 02:17] seed@ubuntu:~/Desktop/md5Collison$ md5sum out2.bin
8ffc37a7b456e7229b3692871039a73b  out2.bin
[06/25/2020 02:17] seed@ubuntu:~/Desktop/md5Collison$
```

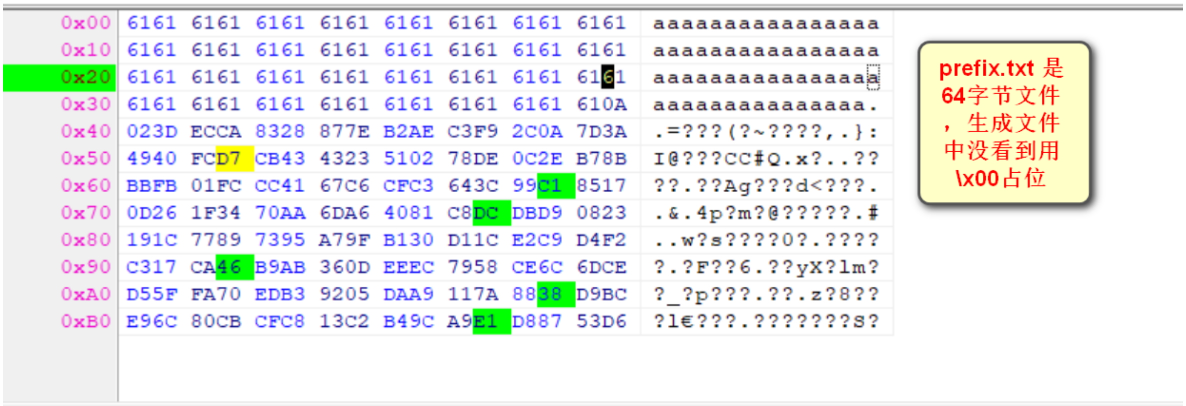
当prefix.txt 文件大小没有达到64字节时



```
0x00  7969 6D75 3139 3939 0A00 0000 0000 0000  yimu1999........
0x10  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x20  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x30  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x40  E947 0329 EABE 6A35 8C53 DC1B DA9B 4850  ?G.)??j5?S?.??HP
0x50  AC2D 68A3 0D59 BBA1 0C1E 42C5 2F34 9FC9  ?-h?.Y??..B?/4??
0x60  A6E5 FEEE 5E48 D5FA 4FE4 C213 2AF6 2BAE  ????^H??O??.*?+?
0x70  2A6D 1E6B AC9C 7DAC 94B8 5C64 CFE7 4A29  *m.k??}???\d??J)
0x80  6572 3613 FABB 6E16 7147 F2DC FF9F 4B27  er6.??n.qG?? ?K'
0x90  9E9C D311 27E6 25A2 D31A 7E3B EC06 DE63  ???.'?%??.~;?.?c
0xA0  062D 9ED5 F494 FC90 7887 50EF D998 E66A  .-??????x?P????j
0xB0  2940 F4A2 AB4C D718 8F0C 1959 BFFC 067D  )@???L?.?..Y??.}
```

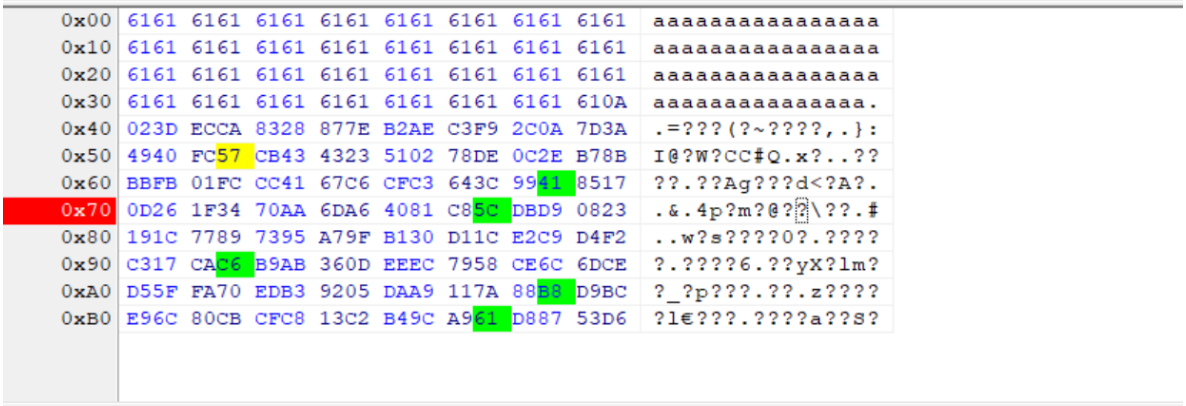
```
0x00  7969 6D75 3139 3939 0A00 0000 0000 0000  yimu1999........
0x10  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x20  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x30  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x40  E947 0329 EABE 6A35 8C53 DC1B DA9B 4850  ?G.)??j5?S?.??HP
0x50  AC2D 6823 0D59 BBA1 0C1E 42C5 2F34 9FC9  ?-h#.Y??..B?/4??
0x60  A6E5 FEEE 5E48 D5FA 4FE4 C213 2A76 2CAE  ????^H??O??.*v,?
0x70  2A6D 1E6B AC9C 7DAC 94B8 5CE4 CFE7 4A29  *m.k??}???\???J)
0x80  6572 3613 FABB 6E16 7147 F2DC FF9F 4B27  er6.??n.qG?? ?K'
0x90  9E9C D391 27E6 25A2 D31A 7E3B EC06 DE63  ????'?%??.~;?.?c
0xA0  062D 9ED5 F494 FC90 7887 50EF D918 E66A  .-??????x?P??.?j
0xB0  2940 F4A2 AB4C D718 8F0C 19D9 BFFC 067D  )@???L?.?..???.}
```

当文件为满64字节时



```
0x00  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x10  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x20  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x30  6161 6161 6161 6161 6161 6161 6161 610A  aaaaaaaaaaaaaaa.
0x40  023D ECCA 8328 877E B2AE C3F9 2C0A 7D3A  .=???(?~????,.}:
0x50  4940 FCD7 CB43 4323 5102 78DE 0C2E B78B  I@???CC#Q.x?..??
0x60  BBFB 01FC CC41 67C6 CFC3 643C 99C1 8517  ??.??Ag???d<???.
0x70  0D26 1F34 70AA 6DA6 4081 C8DC DBD9 0823  .&.4p?m?@?????.#
0x80  191C 7789 7395 A79F B130 D11C E2C9 D4F2  ..w?s????0?.????
0x90  C317 CA46 B9AB 360D EEEC 7958 CE6C 6DCE  ?.?F??6.??yX?lm?
0xA0  D55F FA70 EDB3 9205 DAA9 117A 8838 D9BC  ?_?p???.??.z?8??
0xB0  E96C 80CB CFC8 13C2 B49C A9E1 D887 53D6  ?l€???.???????S?
```

prefix.txt 是64字节文件，生成文件中没看到用\x00占位

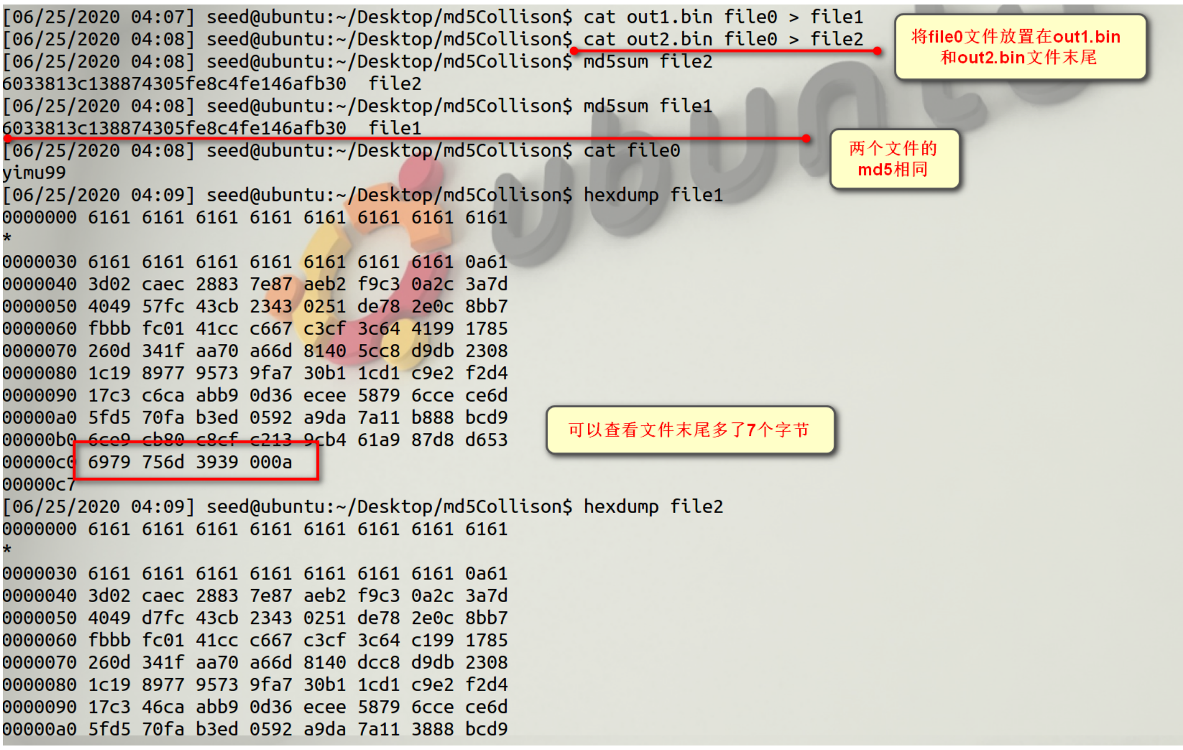


```
0x00  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x10  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x20  6161 6161 6161 6161 6161 6161 6161 6161  aaaaaaaaaaaaaaaa
0x30  6161 6161 6161 6161 6161 6161 6161 610A  aaaaaaaaaaaaaaa.
0x40  023D ECCA 8328 877E B2AE C3F9 2C0A 7D3A  .=???(?~????,.}:
0x50  4940 FC57 CB43 4323 5102 78DE 0C2E B78B  I@?W?CC#Q.x?..??
0x60  BBFB 01FC CC41 67C6 CFC3 643C 9941 8517  ??.??Ag???d<?A?.
0x70  0D26 1F34 70AA 6DA6 4081 C85C DBD9 0823  .&.4p?m?@??\??.#
0x80  191C 7789 7395 A79F B130 D11C E2C9 D4F2  ..w?s????0?.????
0x90  C317 CAC6 B9AB 360D EEEC 7958 CE6C 6DCE  ?.????6.??yX?lm?
0xA0  D55F FA70 EDB3 9205 DAA9 117A 88B8 D9BC  ?_?p???.??.z????
0xB0  E96C 80CB CFC8 13C2 B49C A961 D887 53D6  ?l€???.????a??S?
```

观察到的信息有：当文件大小没有达到64字节时，md5collegn 程序会自动补\0，而达到慢64字节时，只会填满后续的128字节。

而且如上图所示，两文件md5相同时只有6、7个字节不同。

Task 2: Understanding MD5’s Property



```
[06/25/2020 04:07] seed@ubuntu:~/Desktop/md5Collison$ cat out1.bin file0 > file1
[06/25/2020 04:08] seed@ubuntu:~/Desktop/md5Collison$ cat out2.bin file0 > file2
[06/25/2020 04:08] seed@ubuntu:~/Desktop/md5Collison$ md5sum file2
6033813c138874305fe8c4fe146afb30  file2
[06/25/2020 04:08] seed@ubuntu:~/Desktop/md5Collison$ md5sum file1
6033813c138874305fe8c4fe146afb30  file1
[06/25/2020 04:08] seed@ubuntu:~/Desktop/md5Collison$ cat file0
yimu99
[06/25/2020 04:09] seed@ubuntu:~/Desktop/md5Collison$ hexdump file1
0000000 6161 6161 6161 6161 6161 6161 6161 6161
*
0000030 6161 6161 6161 6161 6161 6161 6161 0a61
0000040 3d02 caec 2883 7e87 aeb2 f9c3 0a2c 3a7d
0000050 4049 57fc 43cb 2343 0251 de78 2e0c 8bb7
0000060 fbbb fc01 41cc c667 c3cf 3c64 4199 1785
0000070 260d 341f aa70 a66d 8140 5cc8 d9db 2308
0000080 1c19 8977 9573 9fa7 30b1 1cd1 c9e2 f2d4
0000090 17c3 c6ca abb9 0d36 ecee 5879 6cce ce6d
00000a0 5fd5 70fa b3ed 0592 a9da 7a11 b888 bcd9
00000b0 6ce9 cb80 c8cf c213 9cb4 61a9 87d8 d653
00000c0 6979 756d 3939 000a
00000c7
[06/25/2020 04:09] seed@ubuntu:~/Desktop/md5Collison$ hexdump file2
0000000 6161 6161 6161 6161 6161 6161 6161 6161
*
0000030 6161 6161 6161 6161 6161 6161 6161 0a61
0000040 3d02 caec 2883 7e87 aeb2 f9c3 0a2c 3a7d
0000050 4049 d7fc 43cb 2343 0251 de78 2e0c 8bb7
0000060 fbbb fc01 41cc c667 c3cf 3c64 c199 1785
0000070 260d 341f aa70 a66d 8140 dcc8 d9db 2308
0000080 1c19 8977 9573 9fa7 30b1 1cd1 c9e2 f2d4
0000090 17c3 46ca abb9 0d36 ecee 5879 6cce ce6d
00000a0 5fd5 70fa b3ed 0592 a9da 7a11 3888 bcd9
```

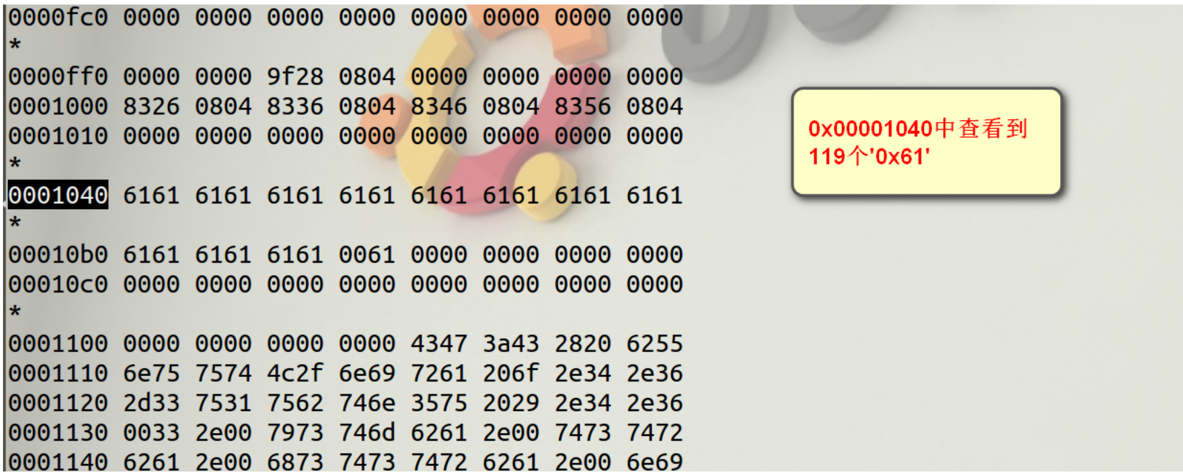
将file0文件放置在out1.bin和out2.bin文件末尾

两个文件的md5相同

可以查看文件末尾多了7个字节

Task 3: Generating Two Executable Files with the Same MD5 Hash

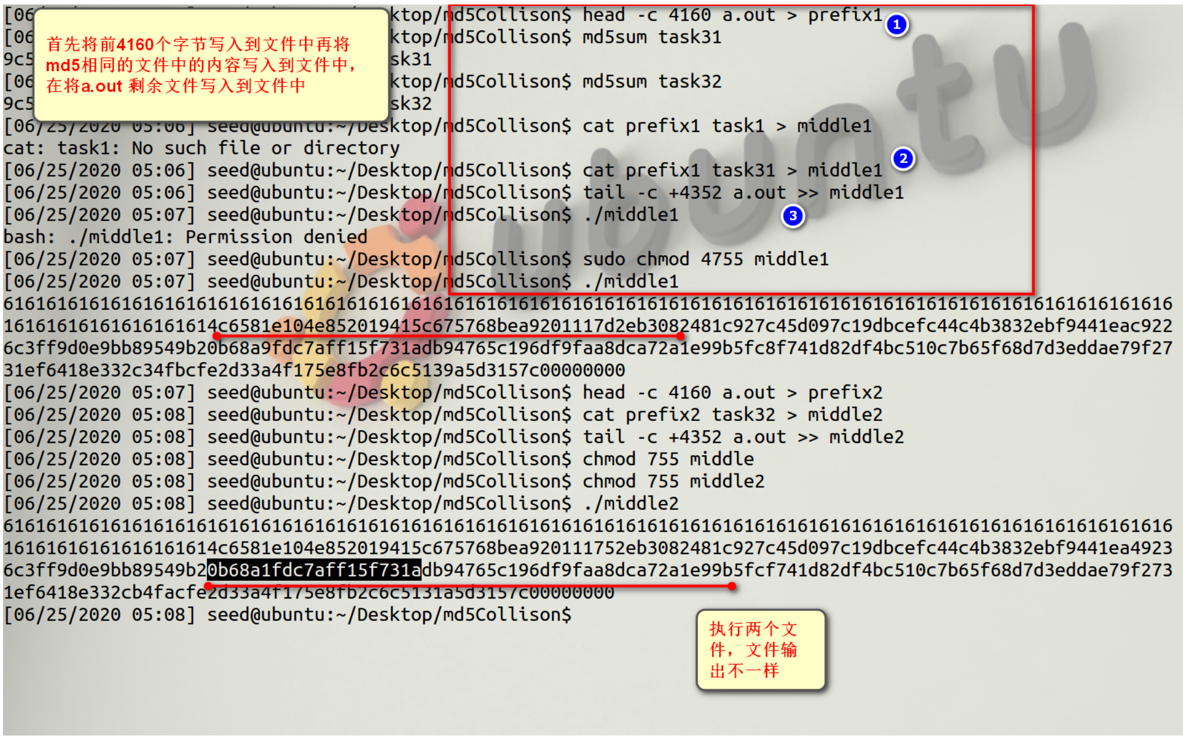
首先找到标记的位置：



```
0000fc0 0000 0000 0000 0000 0000 0000 0000 0000
*
0000ff0 0000 0000 9f28 0804 0000 0000 0000 0000
0001000 8326 0804 8336 0804 8346 0804 8356 0804
0001010 0000 0000 0000 0000 0000 0000 0000 0000
*
0001040 6161 6161 6161 6161 6161 6161 6161 6161
*
00010b0 6161 6161 6161 0061 0000 0000 0000 0000
00010c0 0000 0000 0000 0000 0000 0000 0000 0000
*
0001100 0000 0000 0000 0000 4347 3a43 2820 6255
0001110 6e75 7574 4c2f 6e69 7261 206f 2e34 2e36
0001120 2d33 7531 7562 746e 3575 2029 2e34 2e36
0001130 0033 2e00 7973 746d 6261 2e00 7473 7472
0001140 6261 2e00 6873 7473 7472 6261 2e00 6e69
```

0x00001040中查看到119个'0x61'

再将文件写入



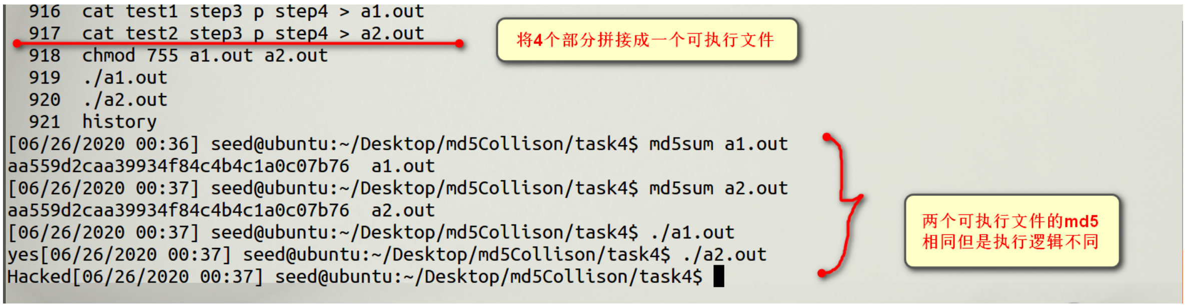
```
[06                                ktop/md5Collison$ head -c 4160 a.out > prefix1
[06                                ktop/md5Collison$ md5sum task31
9c5                                sk31
[06                                ktop/md5Collison$ md5sum task32
9c5                                sk32
[06/25/2020 05:06] seed@ubuntu:~/Desktop/md5Collison$ cat prefix1 task1 > middle1
cat: task1: No such file or directory
[06/25/2020 05:06] seed@ubuntu:~/Desktop/md5Collison$ cat prefix1 task31 > middle1
[06/25/2020 05:06] seed@ubuntu:~/Desktop/md5Collison$ tail -c +4352 a.out >> middle1
[06/25/2020 05:07] seed@ubuntu:~/Desktop/md5Collison$ ./middle1
bash: ./middle1: Permission denied
[06/25/2020 05:07] seed@ubuntu:~/Desktop/md5Collison$ sudo chmod 4755 middle1
[06/25/2020 05:07] seed@ubuntu:~/Desktop/md5Collison$ ./middle1
6161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616
16161616161616161614c6581e104e852019415c675768bea9201117d2eb3082481c927c45d097c19dbcefc44c4b3832ebf9441eac922
6c3ff9d0e9bb89549b20b68a9fdc7aff15f731adb94765c196df9faa8dca72a1e99b5fc8f741d82df4bc510c7b65f68d7d3eddae79f27
31ef6418e332c34fbcfe2d33a4f175e8fb2c6c5139a5d3157c00000000
[06/25/2020 05:07] seed@ubuntu:~/Desktop/md5Collison$ head -c 4160 a.out > prefix2
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$ cat prefix2 task32 > middle2
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$ tail -c +4352 a.out >> middle2
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$ chmod 755 middle
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$ chmod 755 middle2
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$ ./middle2
6161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616161616
16161616161616161614c6581e104e852019415c675768bea920111752eb3082481c927c45d097c19dbcefc44c4b3832ebf9441ea4923
6c3ff9d0e9bb89549b20b68a1fdc7aff15f731adb94765c196df9faa8dca72a1e99b5fcf741d82df4bc510c7b65f68d7d3eddae79f273
1ef6418e332cb4facfe2d33a4f175e8fb2c6c5131a5d3157c00000000
[06/25/2020 05:08] seed@ubuntu:~/Desktop/md5Collison$
```

首先将前4160个字节写入到文件中再将md5相同的文件中的内容写入到文件中，在将a.out 剩余文件写入到文件中

执行两个文件，文件输出不一样

Task 4: Making the Two Programs Behave Differently

执行结果：



```
  916  cat test1 step3 p step4 > a1.out
  917  cat test2 step3 p step4 > a2.out
  918  chmod 755 a1.out a2.out
  919  ./a1.out
  920  ./a2.out
  921  history
[06/26/2020 00:36] seed@ubuntu:~/Desktop/md5Collison/task4$ md5sum a1.out
aa559d2caa39934f84c4b4c1a0c07b76  a1.out
[06/26/2020 00:37] seed@ubuntu:~/Desktop/md5Collison/task4$ md5sum a2.out
aa559d2caa39934f84c4b4c1a0c07b76  a2.out
[06/26/2020 00:37] seed@ubuntu:~/Desktop/md5Collison/task4$ ./a1.out
yes[06/26/2020 00:37] seed@ubuntu:~/Desktop/md5Collison/task4$ ./a2.out
Hacked[06/26/2020 00:37] seed@ubuntu:~/Desktop/md5Collison/task4$ █
```

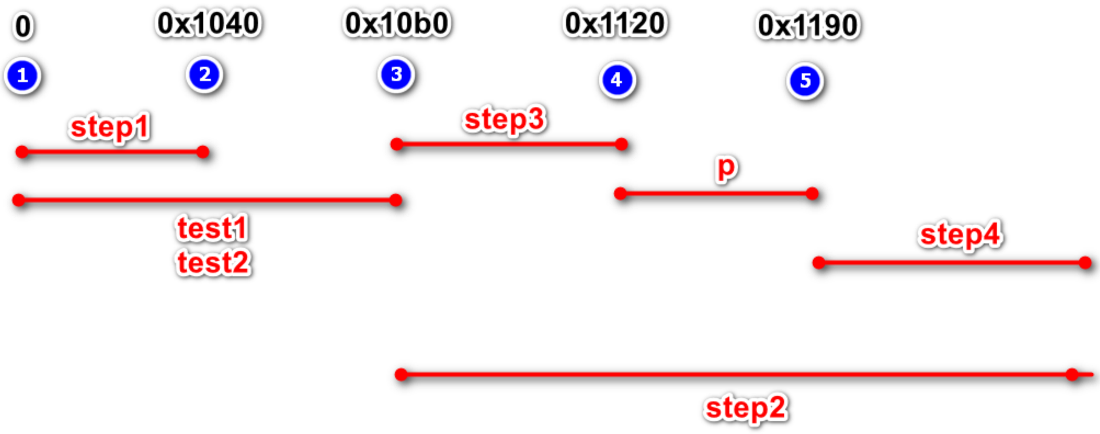
将4个部分拼接成一个可执行文件

两个可执行文件的md5相同但是执行逻辑不同

程序代码

```
#include <stdio.h>
#include <string.h>
char xyz1[200] = {
 'a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a'
};

//占位，为了方便在程序中找了两块aaa的位置
char temp[1000] = {0};

char xyz2[200] = {

 'a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a','a'
};

int main()
{
    int i;
    if(strcmp(xyz1, xyz2) == 0){
        printf("yes");
    }
    else{
        printf("Hacked");
    }

    return 0;
}
```

修改程序流程：


0
0x1040
0x10b0
0x1120
0x1190
1
2
3
4
5
step1
step3
p
test1
test2
step4
step2