Lab4

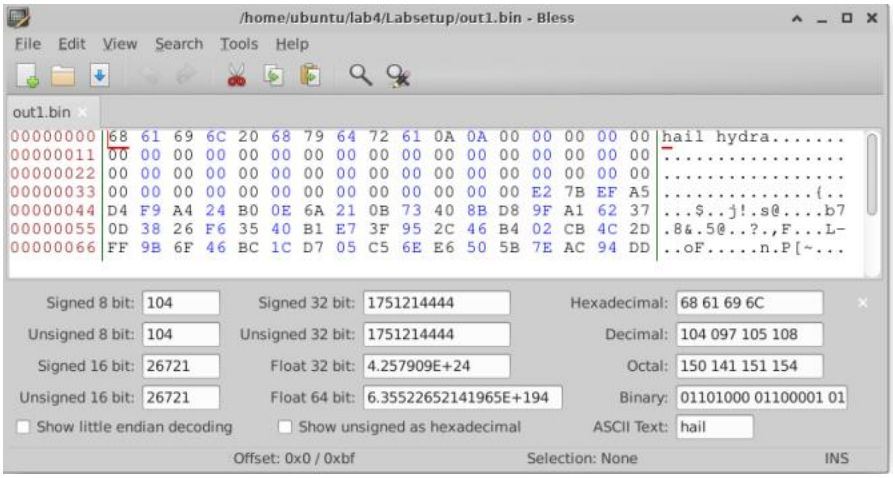
Yue Zhang

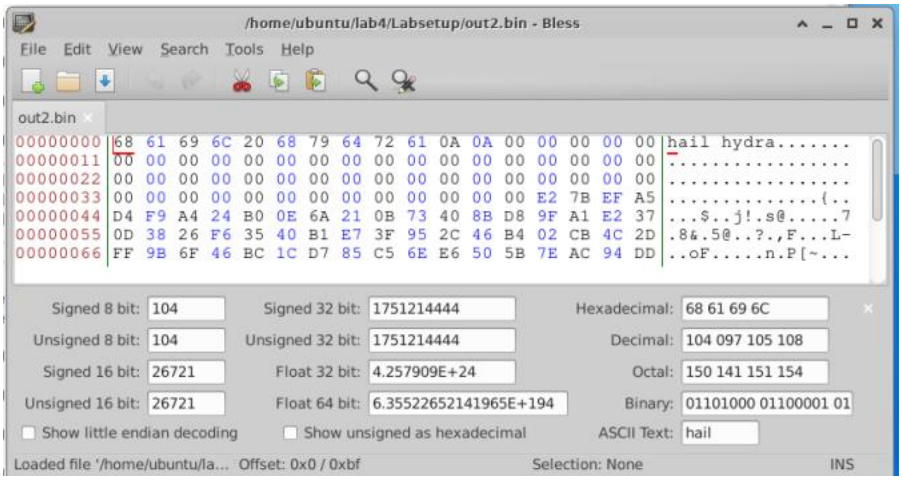
Task1

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ./md5collgen -p prefix.txt -o out1.bin ou
t2.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: 002d1c0f11a2843c3e03457c5f5e4935

Generating first block: .
Generating second block: S11.....................................
Running time: 2.98058 s
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ diff out1.bin out2.bin
Binary files out1.bin and out2.bin differ
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ md5sum out1.bin
97210b75c50656c5b1861604b60c9153  out1.bin
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ md5sum out2.bin
97210b75c50656c5b1861604b60c9153  out2.bin
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$
```

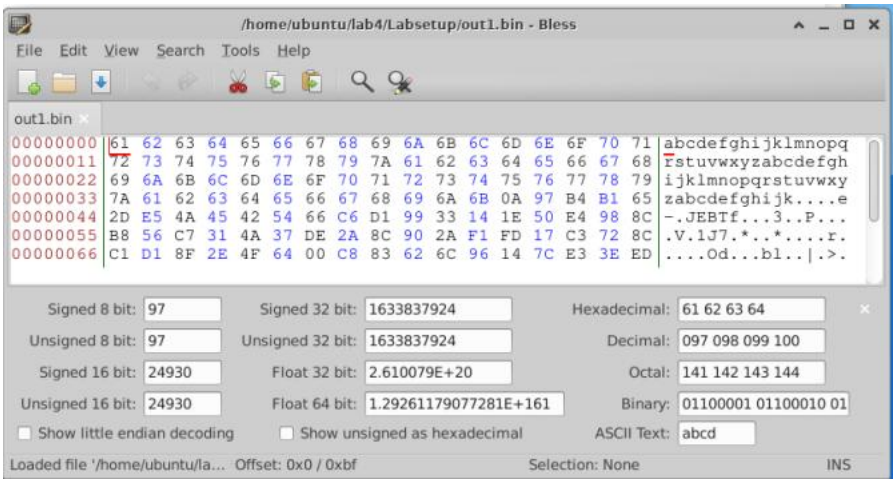


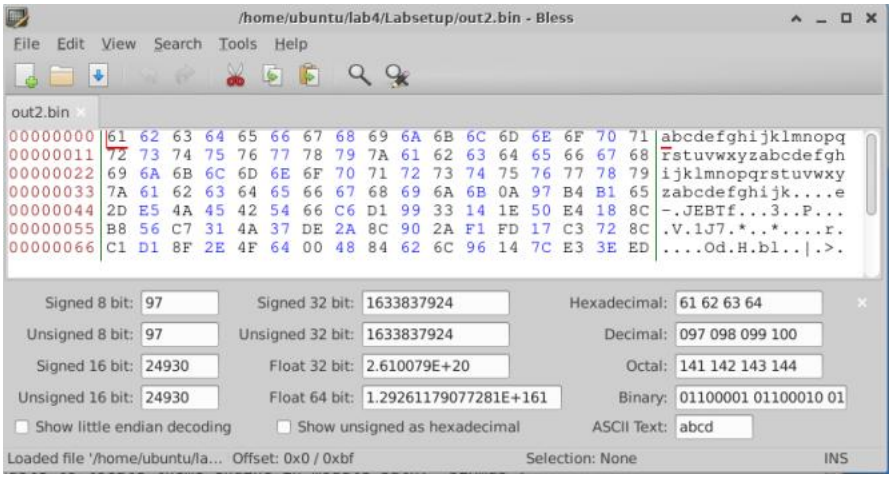


Question1: It will be padded with 00 until file is multiple of 64 bytes.

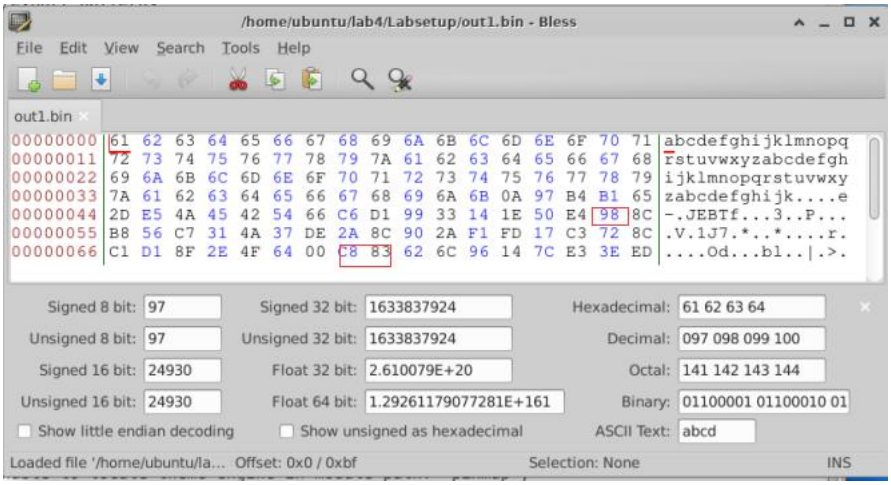
```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ls -l prefix.txt
-rw-rw-r-- 1 seed seed 64 Oct 21 15:07 prefix.txt
```

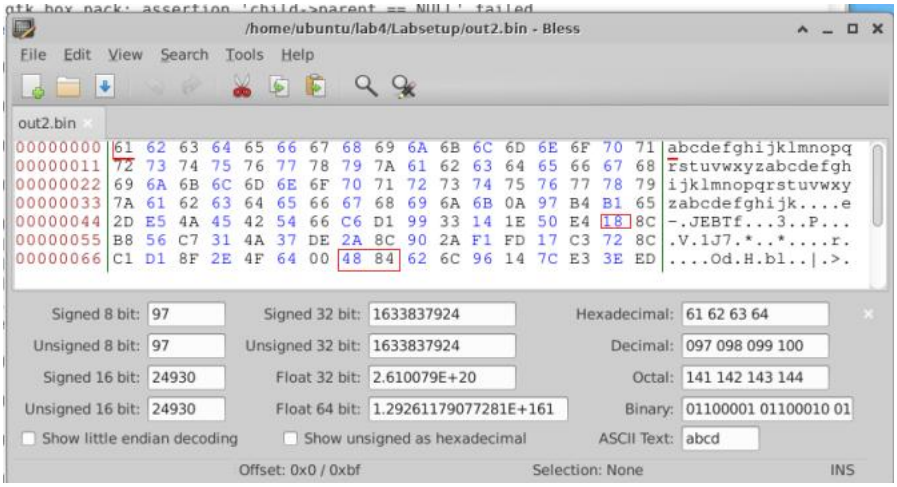
Now, prefix.txt is 64 bytes.





Question2: we noticed there is no padding.





Question3: we noticed that there are three bytes are different.

Task2

```
$ echo hello > out1.bin
$ echo hello > out2.bin
```

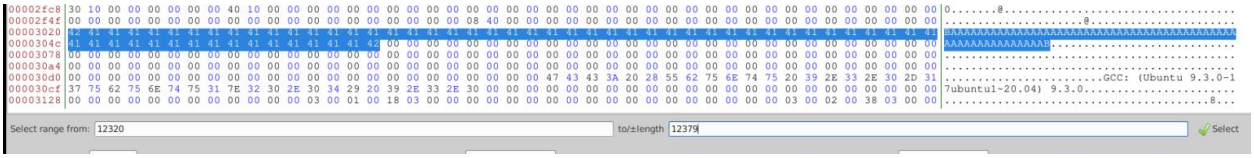
Adding the same suffix to the out1.bin and out2.bin.

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ md5sum out1.bin out2.bin
b1946ac92492d2347c6235b4d2611184  out1.bin
b1946ac92492d2347c6235b4d2611184  out2.bin
```

They have same MD5.

Task3

```
#include <stdio.h>
unsigned char xyz[200] = {
    'B', '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', 'B'
};
int main()
{
    int i;
    for (i=0; i<200; i++){
        printf("%x", xyz[i]);
    }
    printf("\n");
}
~
```



We found the contents are stored in range 12320 to 12379.

```
$ head -c 12340 task3 > prefix
$ tail -c +12353 task3 > suffix
```

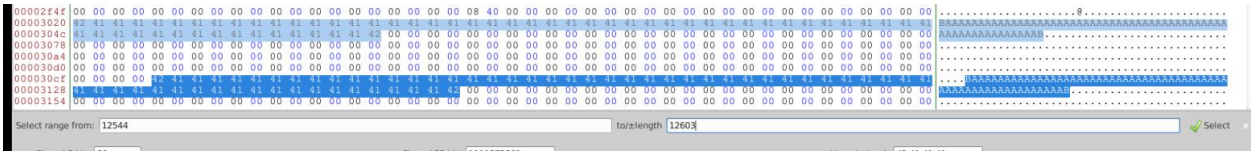
```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ./md5collgen -p prefix -o prefix1 prefix2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'prefix1' and 'prefix2'
Using prefixfile: 'prefix'
Using initial value: 4d2f8dbd74c022581fd4be7cef3ccd49

Generating first block: ..........
Generating second block: S10.....................................................................
........
Running time: 17.7496 s
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ tail -c 128 prefix1 > P
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ tail -c 128 prefix2 > Q
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat prefix P suffix > a1.out
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat prefix Q suffix > a2.out
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ chmod a+x a1.out a2.out
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ diff a1.out a2.out
Binary files a1.out and a2.out differ
```

Task4



The first string is stored in range 12320 to 12379. The second string is stored in range 12544 to 12603.

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ head -c 12340 task4 > prefix
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ./md5collgen -p prefix -o prefix1 prefix2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'prefix1' and 'prefix2'
Using prefixfile: 'prefix'
Using initial value: dab734fb3fa2494f63aa5609153cbf7f

Generating first block: .
Generating second block: W.....
Running time: 0.900154 s
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ tail -c +12768 task4 > suffix
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ tail -c +12320 prefix1 > middle
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ head -c 12543 task4 > tmp1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ tail -c 63 tmp1 > tmp
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat tmp >> prefix1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat tmp >> prefix2
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat middle >> prefix1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat middle >> prefix2
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat tmp >> prefix1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat tmp >> prefix2
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat suffix >> prefix1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ cat suffix >> prefix2
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ chmod a+x prefix1
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ chmod a+x prefix2
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ./prefix1
run benign code
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ ./prefix2
run malicious code
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab4/Labsetup$ md5sum prefix1 prefix2
66f6fe8a6fca59ee3536301e736ad0c0  prefix1
66f6fe8a6fca59ee3536301e736ad0c0  prefix2
```

Prefix1 and prefix2 have the same md5, but they have different result.