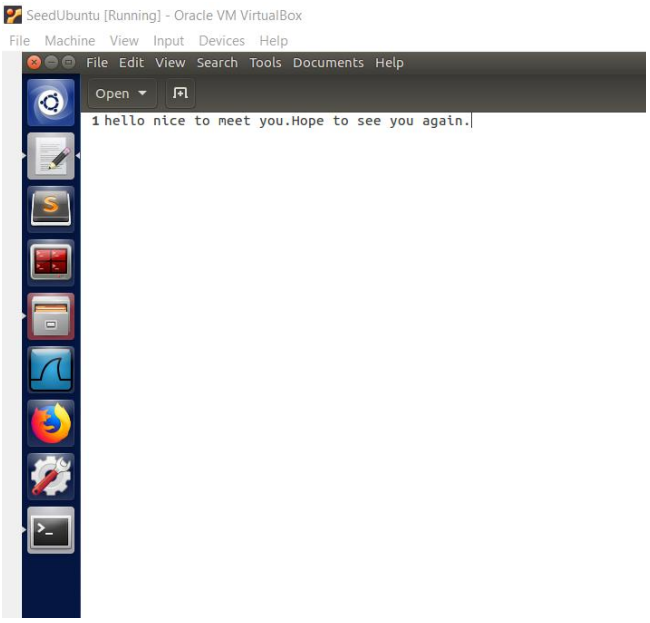
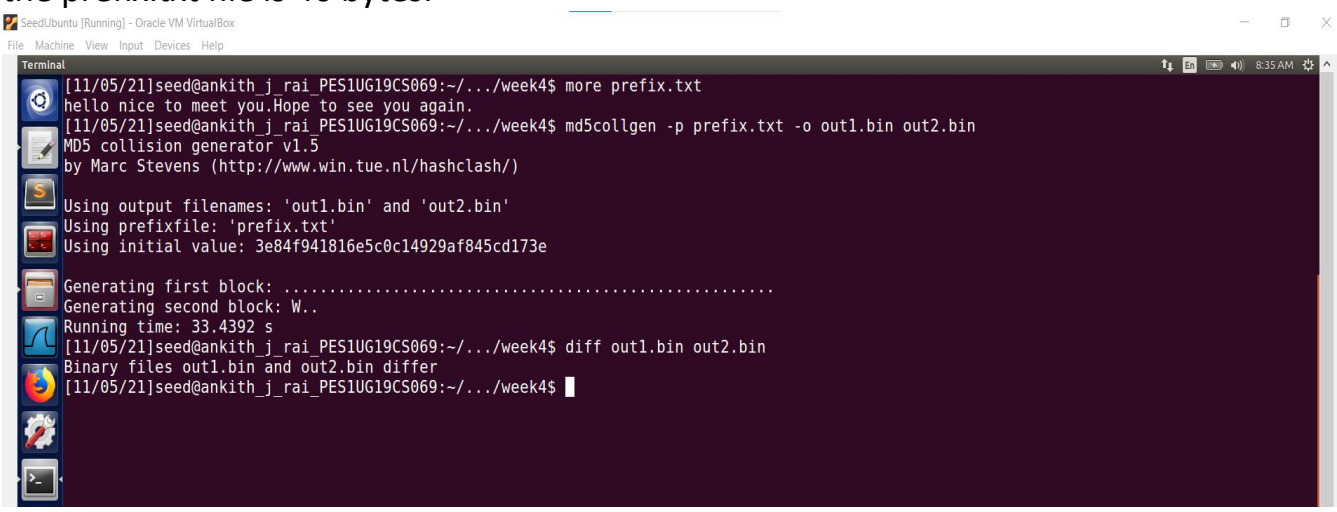
CRYPTOGRAPHY LAB-4
MD5 Collision Attack Lab

NAME : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

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

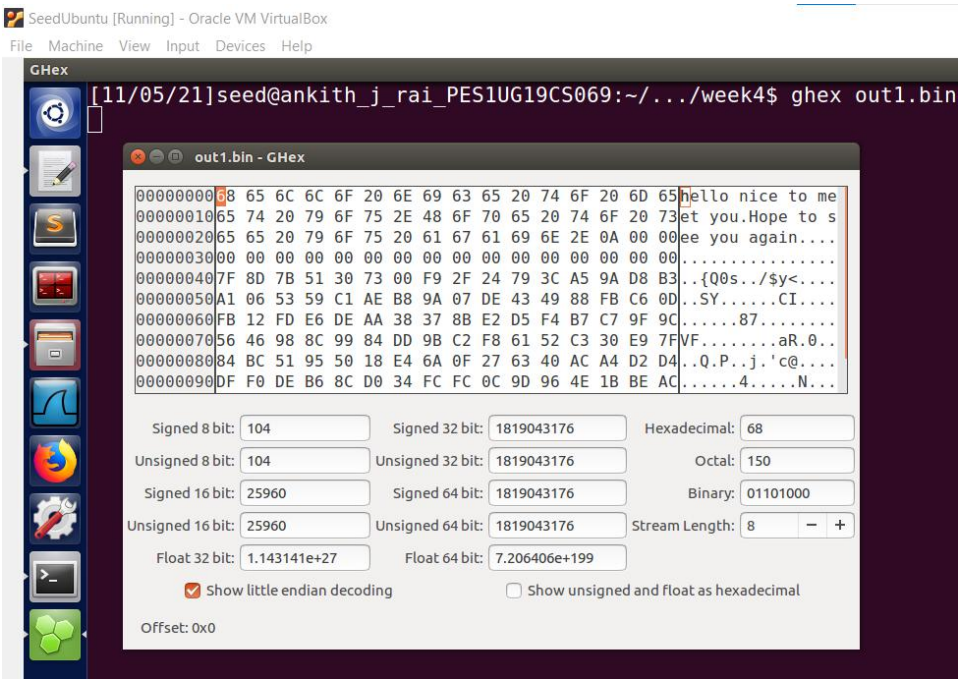


From the above screenshot we can see that I have created a prefix.txt file with contents as shown in the above screenshot. The current size of the prefix.txt file is 46 bytes.

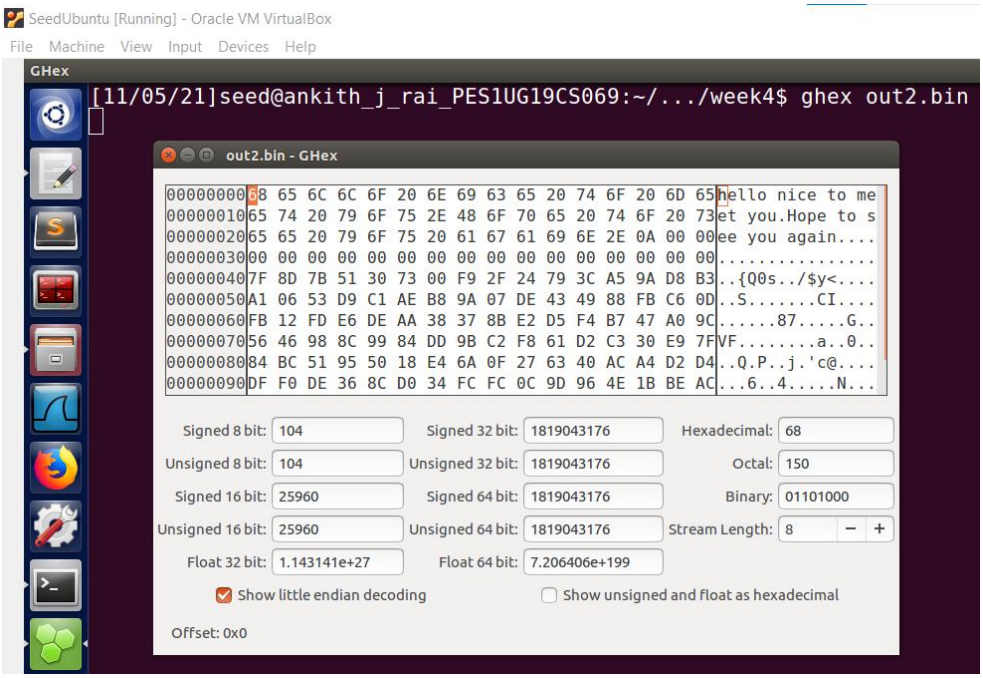


We can see from the above screenshot that we have created two binary output files using prefix.txt and md5collgen. We can also see that the two output files are different from the above screenshot.

Hex output of out1.bin



Hex output of out2.bin

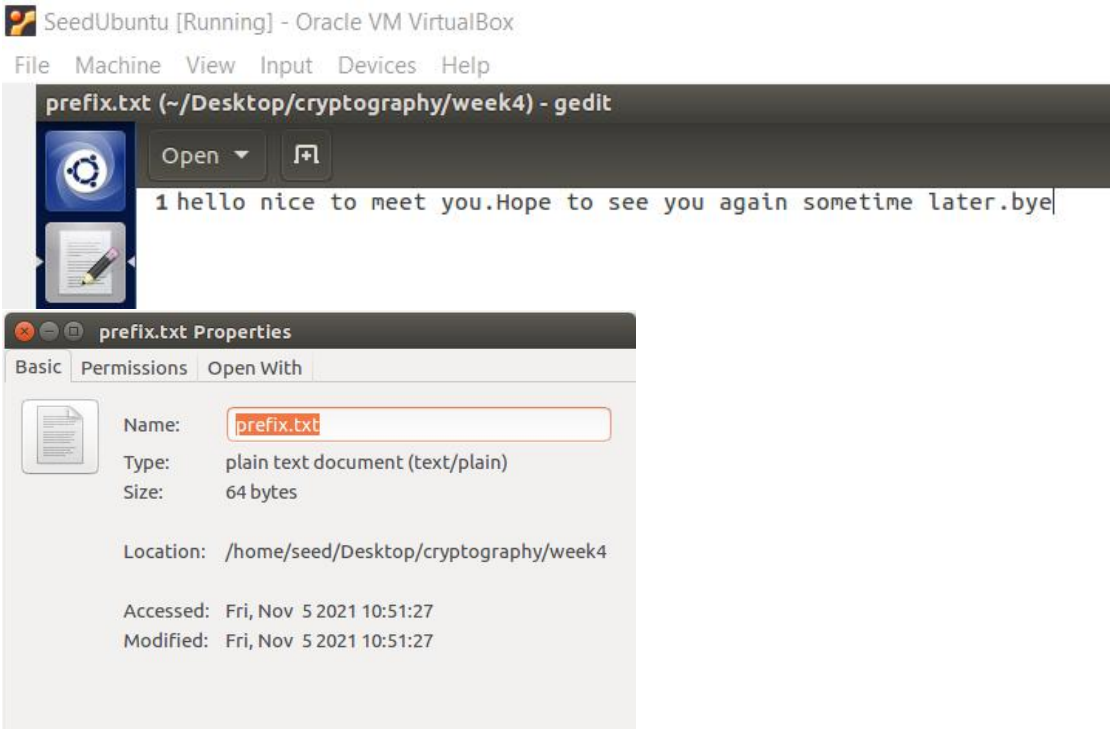


Q1. If the length of your prefix file is not multiple of 64, what is going to happen?

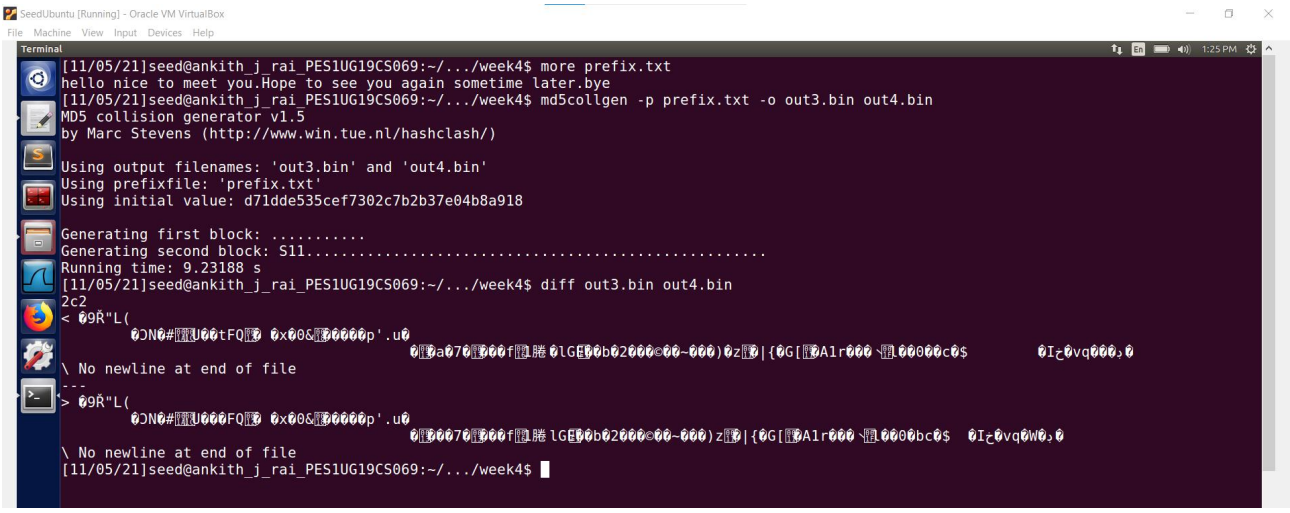
Ans) As we can see that from screenshot it is not a multiple of 64 hence the remaining bits are padded with 0's to make it a multiple of 64.

Q2. Create a prefix file with exactly 64 bytes, and run the tool again, and see what happens.

Ans)



The above screenshot shows that the prefix.txt file is of 64 bytes.

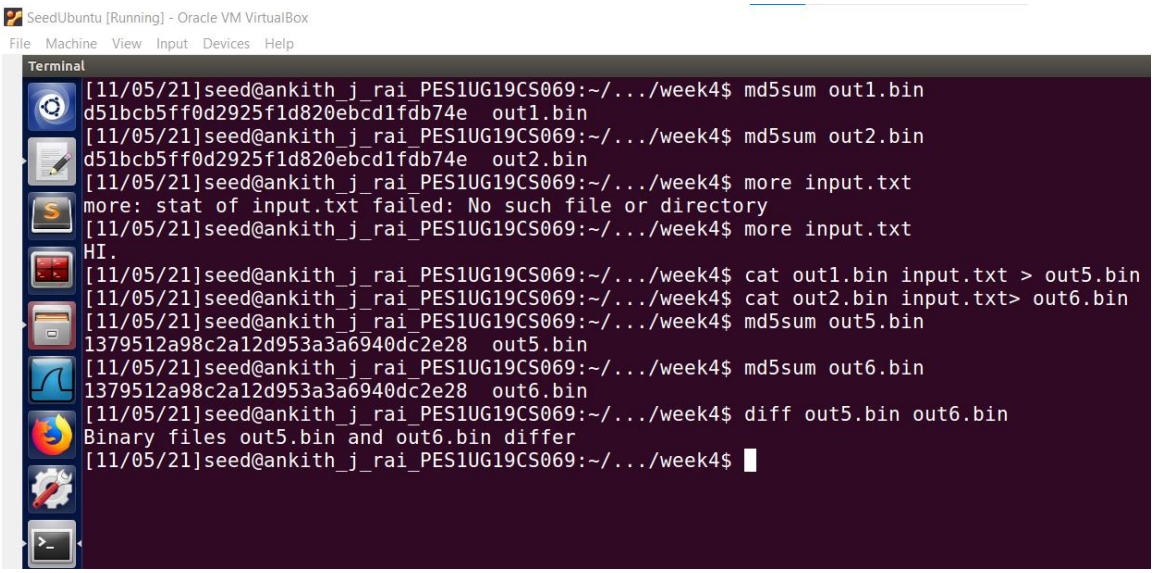


We can see that no padding of 0's is given.

Q3. Are the data generated by md5collgen completely different for the two output files? Please identify and clearly indicate in the screenshots all the bytes that are different (if any).
i) out1.bin and out2.bin ii) out3.bin and out4.bin

Ans)We can see from the screenshot that not all the bytes are different only some are different.

Task 2: Understanding MD5’s property



```
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum out1.bin
d51bcb5ff0d2925f1d820ebcd1fdb74e  out1.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum out2.bin
d51bcb5ff0d2925f1d820ebcd1fdb74e  out2.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ more input.txt
more: stat of input.txt failed: No such file or directory
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ more input.txt
HI.
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ cat out1.bin input.txt > out5.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ cat out2.bin input.txt> out6.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum out5.bin
1379512a98c2a12d953a3a6940dc2e28  out5.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum out6.bin
1379512a98c2a12d953a3a6940dc2e28  out6.bin
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ diff out5.bin out6.bin
Binary files out5.bin and out6.bin differ
[11/05/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ 
```

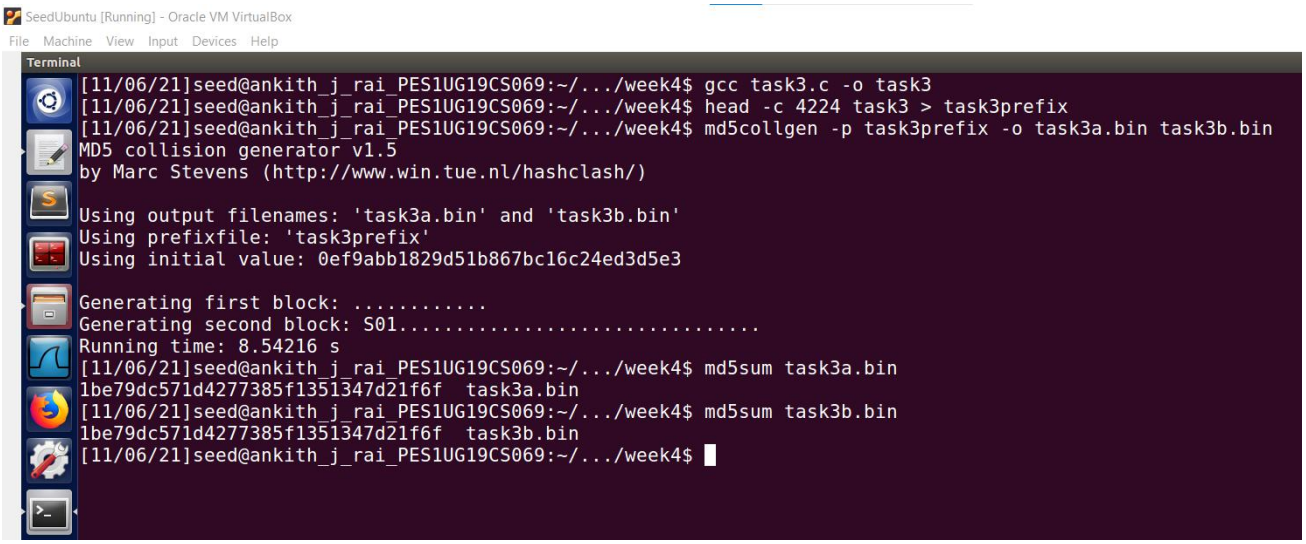
From the above screenshot we can see that both the out1.bin and out2.bin are same .

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

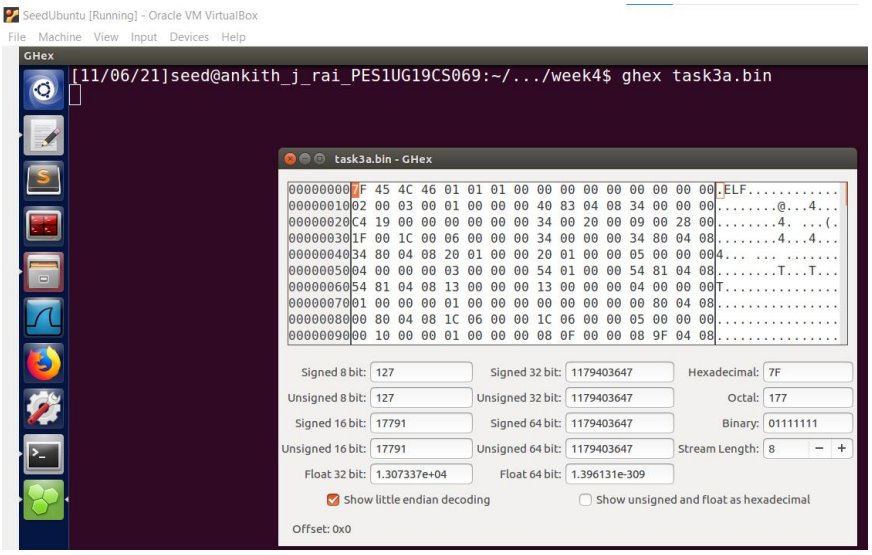
Screenshot of the task3.c file:

```
#include <stdio.h>
unsigned char xyz[400] ={ "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"};
int main()
{
int i;
for (i=0; i<400; i++){
printf("%x", xyz[i]);
}
printf("\n");
}
```

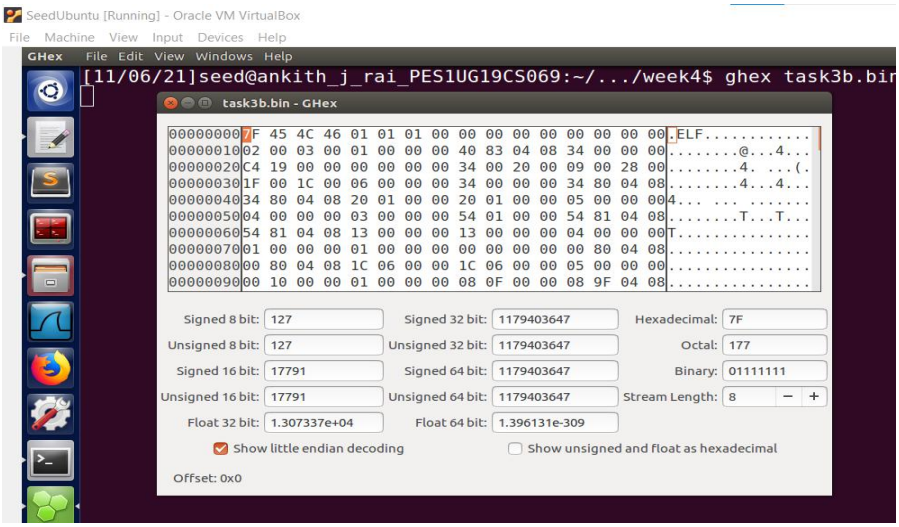
Screenshot of terminal:

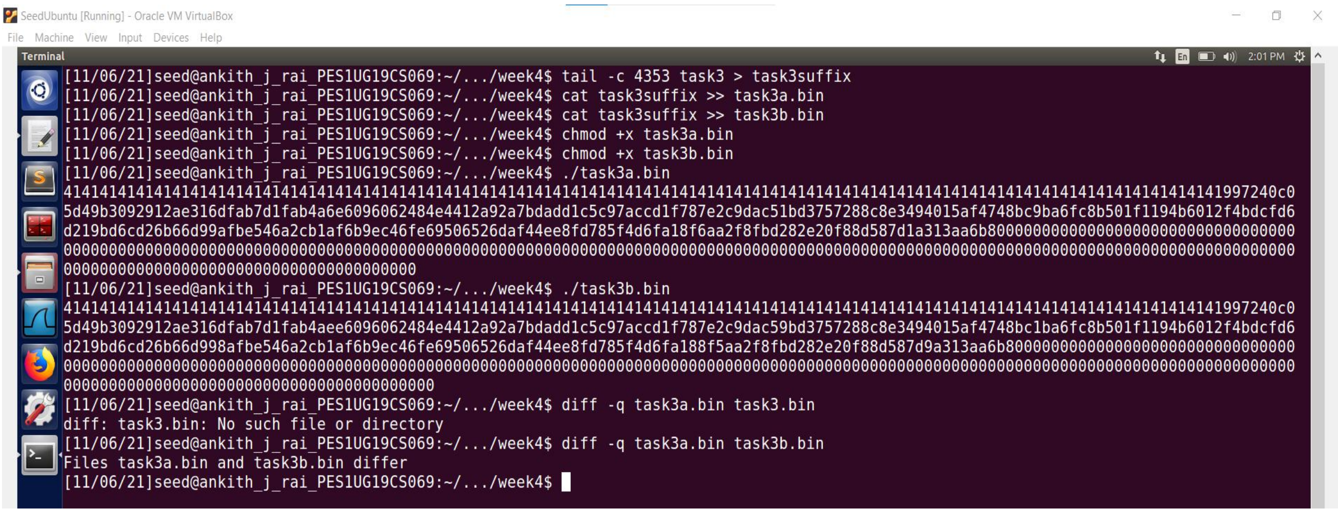


Screenshot of hex editor for task3a.bin



Screenshot of hex editor for task3b.bin





```
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ tail -c 4353 task3 > task3suffix
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ cat task3suffix >> task3a.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ cat task3suffix >> task3b.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ chmod +x task3a.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ chmod +x task3b.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ ./task3a.bin
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141997240c0
5d49b3092912ae316dfab7d1fab4a6e6096062484e4412a92a7bdadd1c5c97accd1f787e2c9dac51bd3757288c8e3494015af4748bc9ba6fc8b501f1194b6012f4bdcfd6
d219bd6cd26b66d99afbe546a2cb1af6b9ec46fe69506526daf44ee8fd785f4d6fa18f6aa2f8fbd282e20f88d587d1a313aa6b8000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ ./task3b.bin
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141997240c0
5d49b3092912ae316dfab7d1fab4aee6096062484e4412a92a7bdadd1c5c97accd1f787e2c9dac59bd3757288c8e3494015af4748bc1ba6fc8b501f1194b6012f4bdcfd6
d219bd6cd26b66d998afbe546a2cb1af6b9ec46fe69506526daf44ee8fd785f4d6fa188f5aa2f8fbd282e20f88d587d9a313aa6b800000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ diff -q task3a.bin task3.bin
diff: task3.bin: No such file or directory
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ diff -q task3a.bin task3b.bin
Files task3a.bin and task3b.bin differ
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ 
```

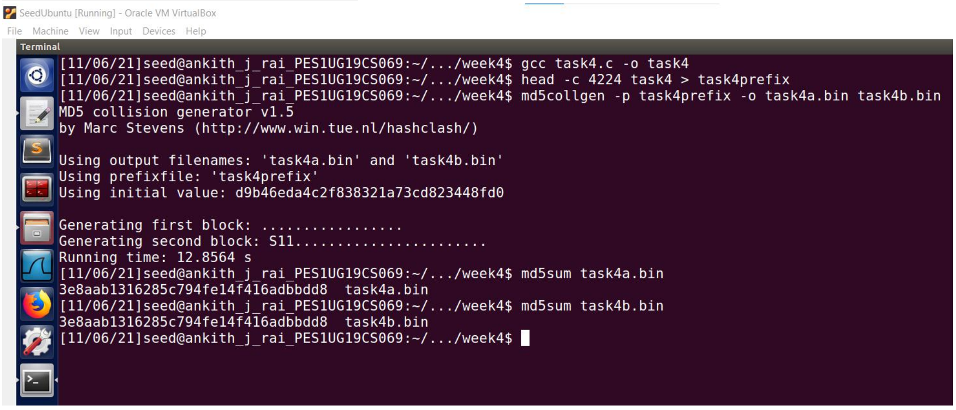
We can see that task3a.bin and task3b.bin differ from each other.

Task 4: Making the two programs behave Differently

Screenshot of the task3.c file:

```
#include <stdio.h>
unsigned char X[400] = {"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"};
unsigned char Y[400] = {"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"};
int a=0;
int main()
{
 for (int i=0; i<400; i++)
 {
if( X[i] == Y[i] )
continue;
else
{
 a=1;
 break;
}
 }
 if(a==0)
printf("Good\n");
 else
 printf("Bad\n");
}
```

Screenshot of terminal:

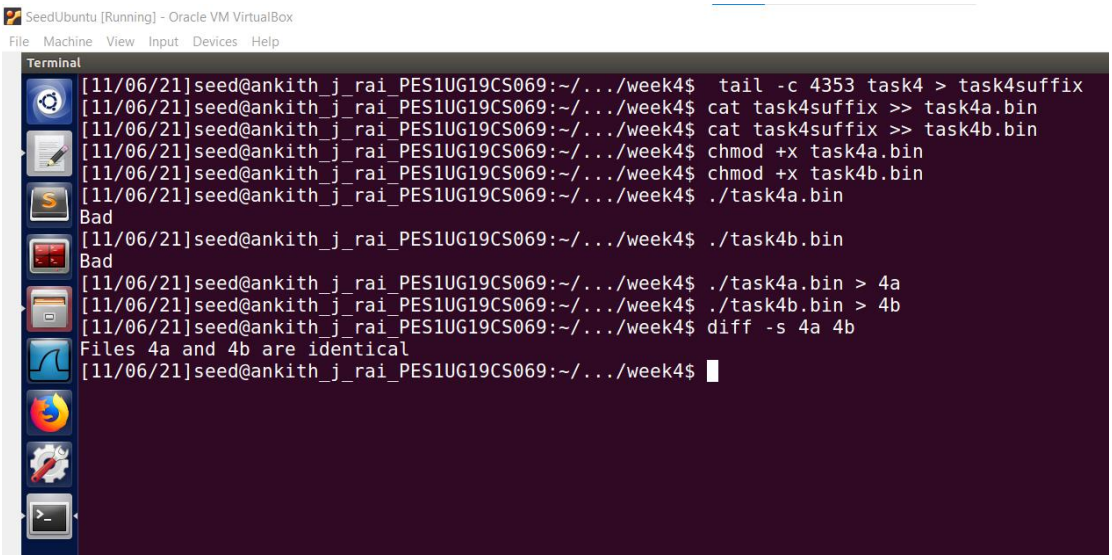


```
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ gcc task4.c -o task4
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ head -c 4224 task4 > task4prefix
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5collgen -p task4prefix -o task4a.bin task4b.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'task4a.bin' and 'task4b.bin'
Using prefixfile: 'task4prefix'
Using initial value: d9b46eda4c2f838321a73cd823448fd0

Generating first block: .................
Generating second block: S11.......................
Running time: 12.8564 s
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum task4a.bin
3e8aab1316285c794fe14f416adbbdd8  task4a.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ md5sum task4b.bin
3e8aab1316285c794fe14f416adbbdd8  task4b.bin
[11/06/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week4$ 
```

From the above screenshot we can see that md5sum of both task4a.bin and task4b.bin is same.



We can see from the above screenshot that after running task4a.bin and task4b.bin we get the output as Bad.

Even after appending content’s to the 4a and 4b they remain identical.