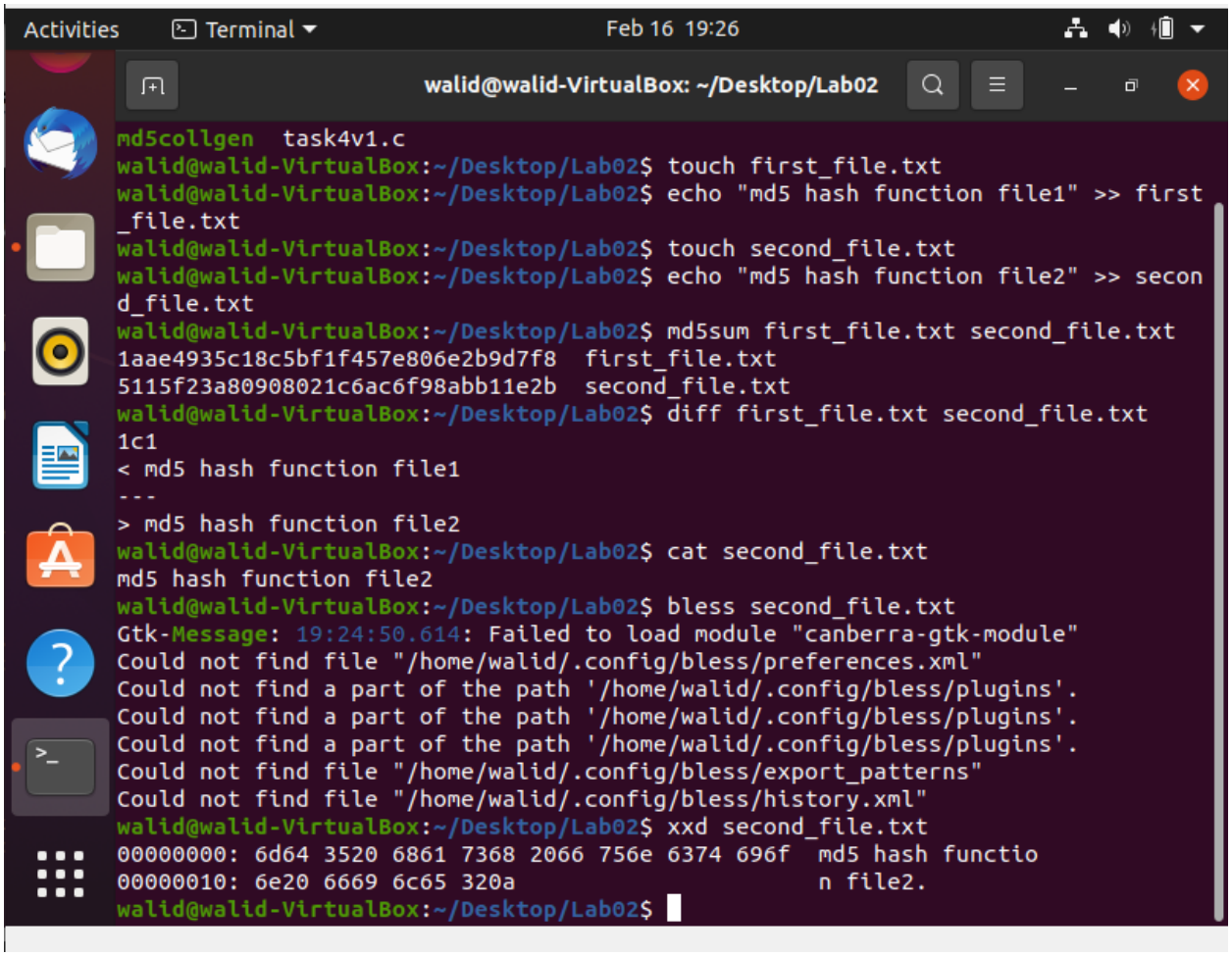
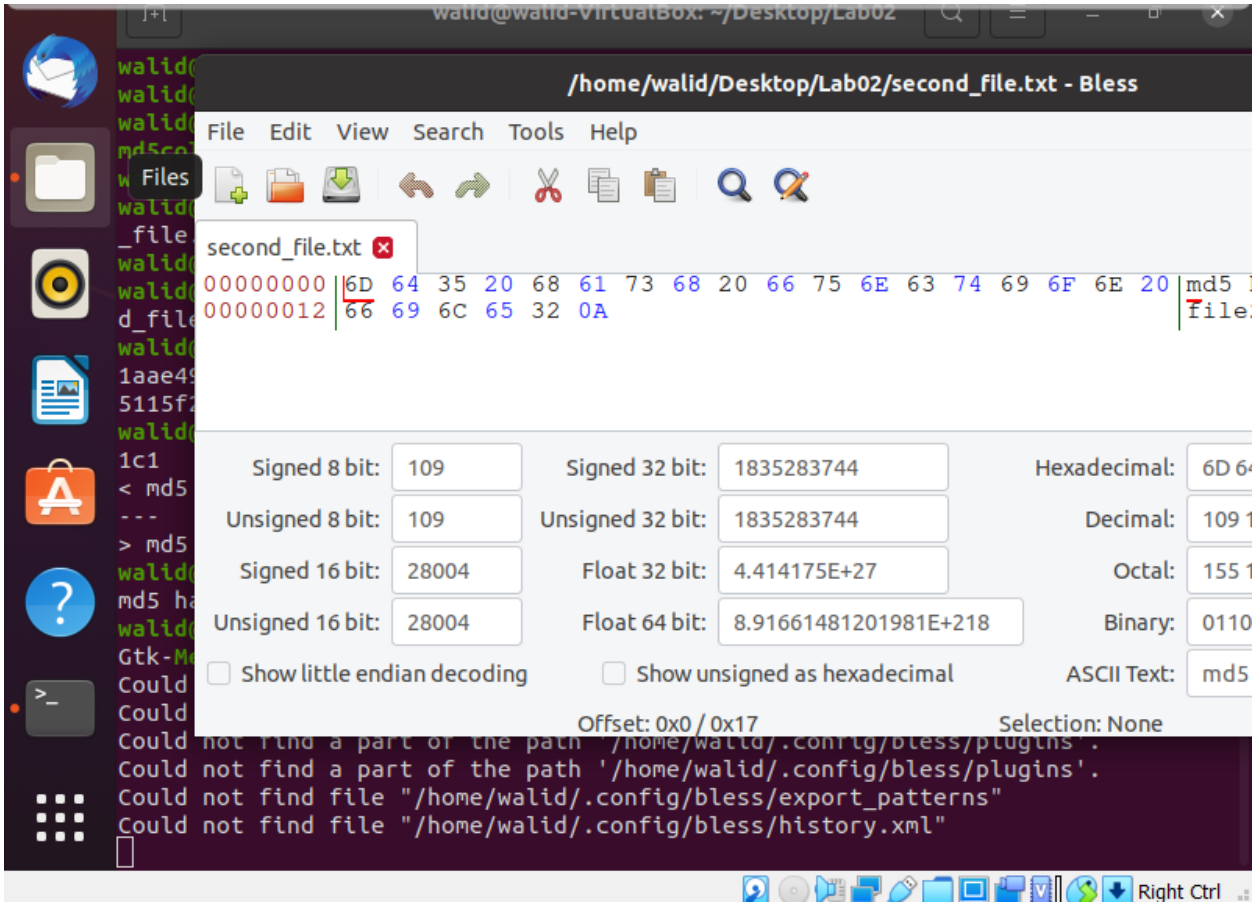
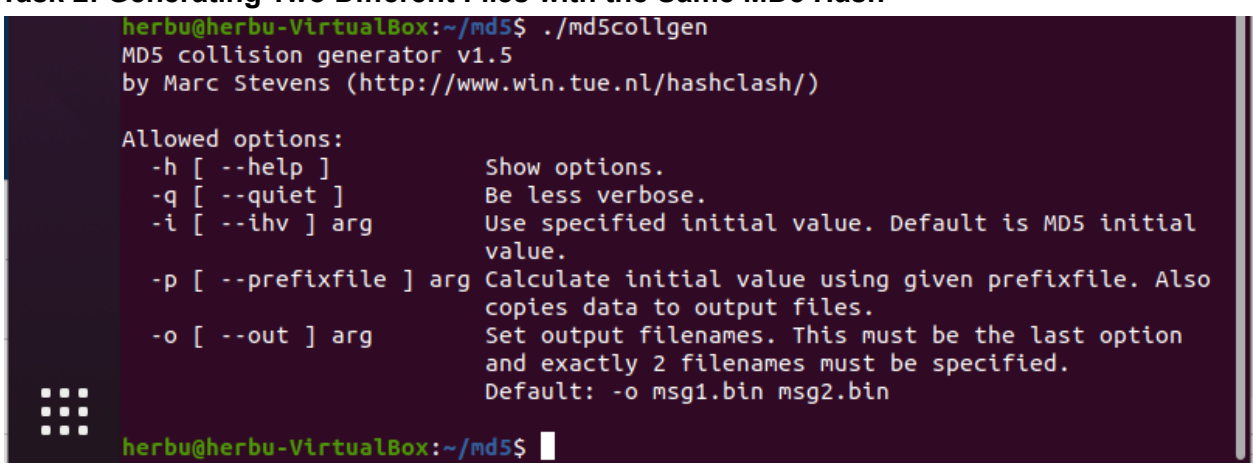
Lab #02 – Md5 collision
Lab Group 13
Kalid Ajibade (100660188)
Walid Ayub (100695612)
Zain Butt (100751676)
Konrad Herbus (100768380)

Task 1: Can two different files have the same md5 hash?



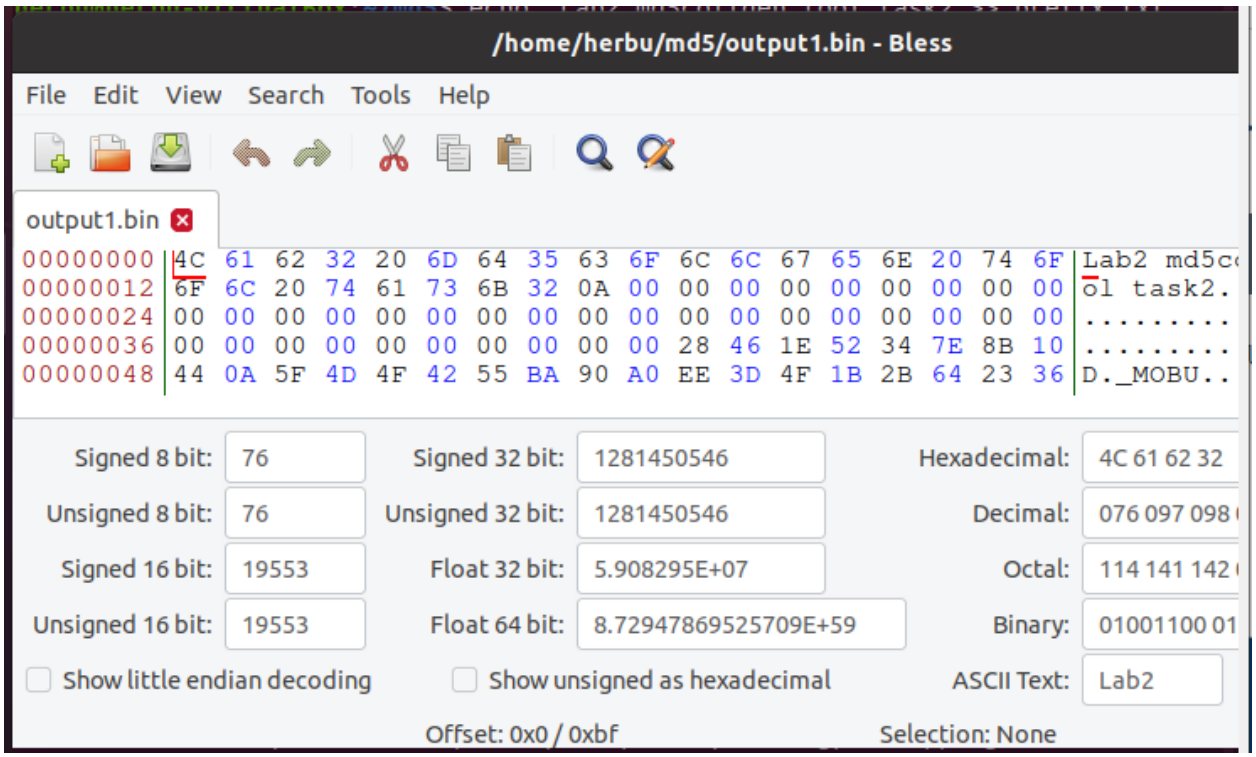


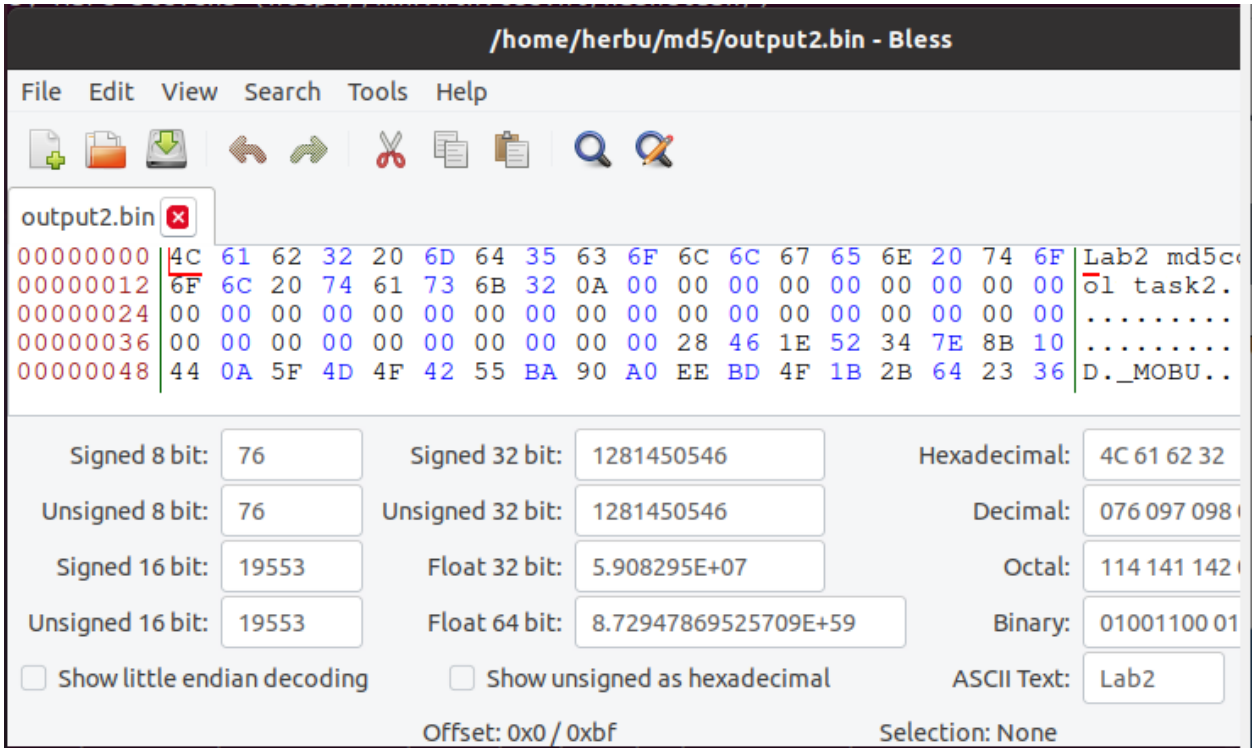
Task 2: Generating Two Different Files with the Same MD5 Hash



```
herbu@herbu-VirtualBox:~/md5$ ./md5collgen
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Allowed options:
  -h [ --help ]           Show options.
  -q [ --quiet ]          Be less verbose.
  -i [ --ihv ] arg        Use specified initial value. Default is MD5 initial
                          value.
  -p [ --prefixfile ] arg Calculate initial value using given prefixfile. Also
                          copies data to output files.
  -o [ --out ] arg        Set output filenames. This must be the last option
                          and exactly 2 filenames must be specified.
                          Default: -o msg1.bin msg2.bin

herbu@herbu-VirtualBox:~/md5$
```

```
herbu@herbu-VirtualBox:~/md5$ touch prefix.txt
herbu@herbu-VirtualBox:~/md5$ echo "Lab2 md5collgen tool task2">> prefix.txt
herbu@herbu-VirtualBox:~/md5$ cat prefix.txt
Lab2 md5collgen tool task2
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p prefix.txt -o output1.bin output2
.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'output1.bin' and 'output2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: 5cdc89c18539641a00395fd8a171a976

Generating first block: ...........
Generating second block: S00....
Running time: 7.37672 s
herbu@herbu-VirtualBox:~/md5$ ls *.bin
output1.bin  output2.bin
herbu@herbu-VirtualBox:~/md5$ diff output1.bin output2.bin
Binary files output1.bin and output2.bin differ
```






```
herbu@herbu-VirtualBox:~/md5$ xxd output1.bin
00000000: 4c61 6232 206d 6435 636f 6c6c 6765 6e20  Lab2 md5collgen
00000010: 746f 6f6c 2074 6173 6b32 0a00 0000 0000  tool task2......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: 2846 1e52 347e 8b10 440a 5f4d 4f42 55ba  (F.R4~..D._MOBU.
00000050: 90a0 ee3d 4f1b 2b64 2336 3be5 a930 3238  ...=O.+d#6;..028
00000060: 0cc6 ad0e 6006 8a46 6b06 6bf3 c9db 693c  ....`..Fk.k...i<
00000070: 909c f39d da1a b481 4bf2 2634 7da5 99fe  ........K.&4}...
00000080: 62f6 ccfc 800d 81b9 a5c9 a225 019b b34d  b..........%...M
00000090: 3a36 7502 fff4 001a d117 f7cc d031 5932  :6u..........1Y2
000000a0: b320 1fd6 1ead 8167 cda9 a0ef a4e2 7baa  . .....g......{.
000000b0: 9bbb c781 e296 adde 3193 388e 81e8 1050  ........1.8....P
```

```
herbu@herbu-VirtualBox:~/md5$ md5sum output1.bin
8c1473dafdef304c4a9747d28b85f179  output1.bin
```

Q1: Create a prefix file where the length of your prefix file is not multiple of 64 bytes, run the collision tool, and then use the hex editor to share your insights.

```
herbu@herbu-VirtualBox:~/md5$ echo " Lab2 md5collgen tool task2">> prefix_1.txt
herbu@herbu-VirtualBox:~/md5$ cat prefix_1.txt
 Lab2 md5collgen tool task2
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p prefix_1.txt -o out_1.bin out_2.b
in
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out_1.bin' and 'out_2.bin'
Using prefixfile: 'prefix_1.txt'
Using initial value: dbaed06ae1161884024d6ee76913a6d9

Generating first block: ...
Generating second block: S11.................
Running time: 3.75909 s
```

Q2. Create a prefix file with exactly 64 bytes, run the collision tool, and then use the hex editor to share your insights

```
herbu@herbu-VirtualBox:~/md5$ echo $(python3 -c 'print("A"*63)') >> prefix_64.t
xt
herbu@herbu-VirtualBox:~/md5$ cat prefix_64.txt

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
herbu@herbu-VirtualBox:~/md5$ ls -l *.txt
-rw-rw-r-- 1 herbu herbu 28 Feb 14 13:01 prefix_1.txt
-rw-rw-r-- 1 herbu herbu 65 Feb 14 13:04 prefix_64.txt
-rw-rw-r-- 1 herbu herbu 27 Feb 14 12:48 prefix.txt
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p prefix_64.txt -o out11.bin out_22
.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out11.bin' and 'out_22.bin'
Using prefixfile: 'prefix_64.txt'
Using initial value: d46b988132ccf1a01611c6fb99de1691

Generating first block: ....................................
Generating second block: S01....................
Running time: 27.9419 s
```

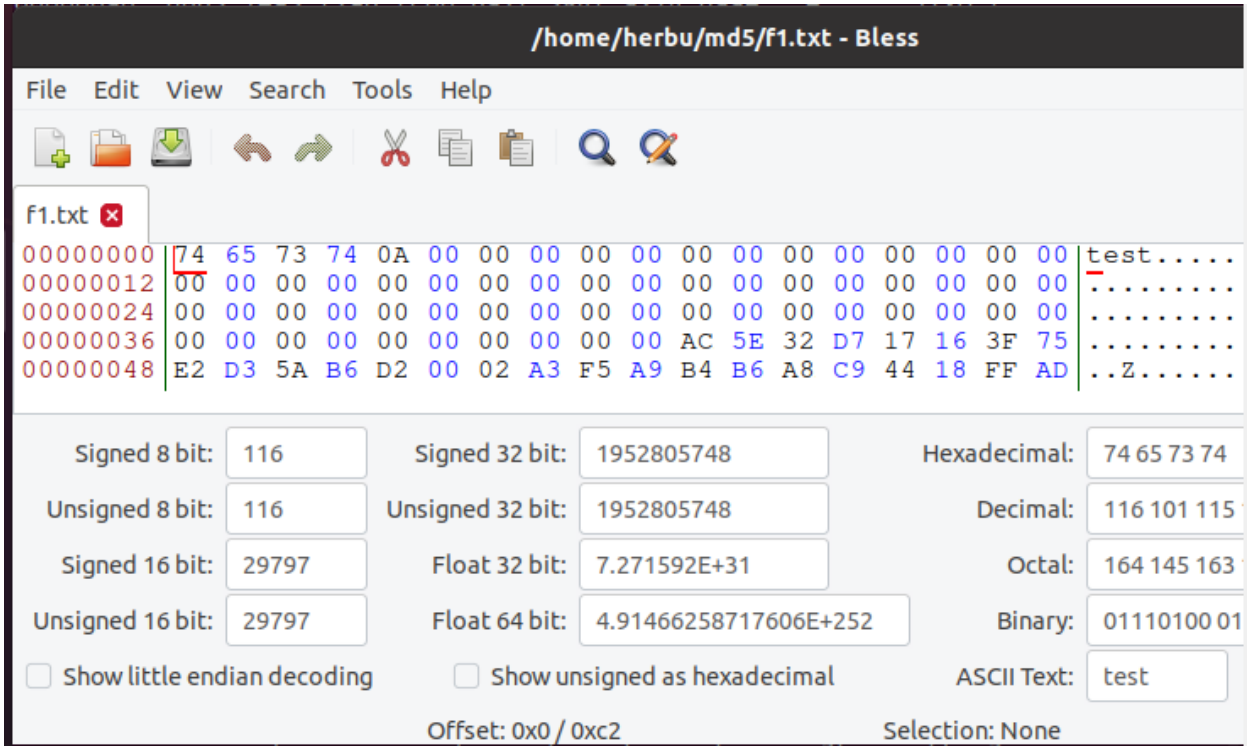
Task 3: Understanding MD5's Property

```
herbu@herbu-VirtualBox:~/md5$ echo "test" >> hello.txt
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p hello.txt -o f1.txt f2.txt
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'f1.txt' and 'f2.txt'
Using prefixfile: 'hello.txt'
Using initial value: ad312f555a16d0ea0cbc1728101ca9a9

Generating first block: .
Generating second block: S01.
Running time: 0.594695 s
herbu@herbu-VirtualBox:~/md5$ md5sum f1.txt f2.txt
35ef2426f4841b125edd4a6b1863a819  f1.txt
35ef2426f4841b125edd4a6b1863a819  f2.txt
herbu@herbu-VirtualBox:~/md5$ diff f1.txt f2.txt
Binary files f1.txt and f2.txt differ
```

```
herbu@herbu-VirtualBox:~/md5$ xxd f1.txt
00000000: 7465 7374 0a00 0000 0000 0000 0000 0000  test............
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: ac5e 32d7 1716 3f75 e2d3 5ab6 d200 02a3  .^2...?u..Z.....
00000050: f5a9 b4b6 a8c9 4418 ffad 3972 090a 0bc6  ......D...9r....
00000060: cc01 0af4 cc2d d786 6fd0 5b14 b79d 197f  .....-..o.[.....
00000070: 9df9 89b6 5269 8568 4709 6b68 ac27 4584  ....Ri.hG.kh.'E.
00000080: a28f 6c0a 0887 5bff c1e8 5c20 270c a41a  ..l...[...\ '...
00000090: 281f 1927 f785 46b3 d31a 0648 ecc7 dd6b  (..'..F....H...k
000000a0: d065 1e95 f296 fc00 6a2f 584f a274 daae  .e......j/XO.t..
000000b0: 39f0 3f3c a96b 240c 1bde a706 7fab 3cf6  9.?<.k$.......<.
herbu@herbu-VirtualBox:~/md5$ xxd f2.txt
00000000: 7465 7374 0a00 0000 0000 0000 0000 0000  test............
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: ac5e 32d7 1716 3f75 e2d3 5ab6 d200 02a3  .^2...?u..Z.....
00000050: f5a9 b436 a8c9 4418 ffad 3972 090a 0bc6  ...6..D...9r....
00000060: cc01 0af4 cc2d d786 6fd0 5b14 b71d 1a7f  .....-..o.[.....
00000070: 9df9 89b6 5269 8568 4709 6be8 ac27 4584  ....Ri.hG.k..'E.
00000080: a28f 6c0a 0887 5bff c1e8 5c20 270c a41a  ..l...[...\ '...
00000090: 281f 19a7 f785 46b3 d31a 0648 ecc7 dd6b  (.....F....H...k
000000a0: d065 1e95 f296 fc00 6a2f 584f a2f4 d9ae  .e......j/XO....
000000b0: 39f0 3f3c a96b 240c 1bde a786 7fab 3cf6  9.?<.k$.......<.
```

```
herbu@herbu-VirtualBox:~/md5$ echo hi>> f1.txt
herbu@herbu-VirtualBox:~/md5$ echo hi>> f2.txt
herbu@herbu-VirtualBox:~/md5$ md5sum f1.txt f2.txt
40ff7b8af5381724480a5add39bf45bd  f1.txt
40ff7b8af5381724480a5add39bf45bd  f2.txt
```

```
herbu@herbu-VirtualBox:~/md5$ echo "test" >> f11.txt
herbu@herbu-VirtualBox:~/md5$ bless f1.txt
```

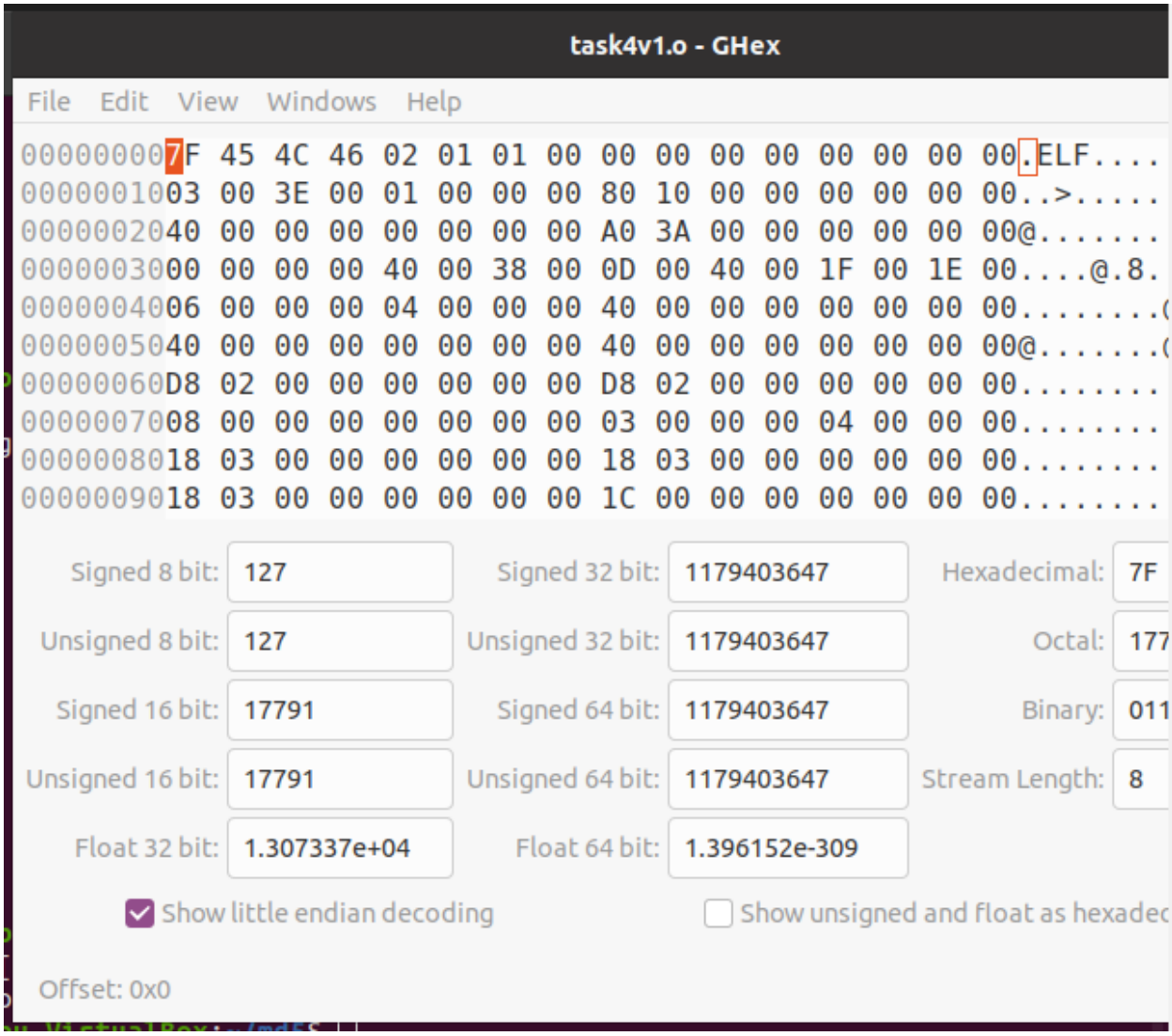



```
herbu@herbu-VirtualBox:~/md5$ echo "test" >> f22.txt
herbu@herbu-VirtualBox:~/md5$ md5sum f11.txt f22.txt
d8e8fca2dc0f896fd7cb4cb0031ba249  f11.txt
d8e8fca2dc0f896fd7cb4cb0031ba249  f22.txt
herbu@herbu-VirtualBox:~/md5$ diff f11.txt f22.txt
herbu@herbu-VirtualBox:~/md5$ echo "codes" >> f3.txt
```

```
herbu@herbu-VirtualBox:~/md5$ cat f11.txt f3.txt > f111.txt
herbu@herbu-VirtualBox:~/md5$ cat f22.txt f3.txt > f222.txt
herbu@herbu-VirtualBox:~/md5$ md5sum f111.txt f222.txt
11428c9aaef5267729b40190b5d417c8  f111.txt
11428c9aaef5267729b40190b5d417c8  f222.txt
herbu@herbu-VirtualBox:~/md5$ md5sum f11.txt f22.txt
d8e8fca2dc0f896fd7cb4cb0031ba249  f11.txt
d8e8fca2dc0f896fd7cb4cb0031ba249  f22.txt
```

Task 4: Generating Two Executable Files with the Same MD5 Hash

```
herbu@herbu-VirtualBox:~/md5$ gcc task4v1.c -o task4v1.o
herbu@herbu-VirtualBox:~/md5$ ./task4v1.o
414141414141414141414141414141414141414141414141414141414141414141414141414141414
141414141414141414141414141414141414141414141414141414141414141414141414141414141
414141414141414141414141414141414141414141414141414141414141414141414141414141414
141414141414141414141414141414141414141414141414141414141414141414141414141414141
414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141
herbu@herbu-VirtualBox:~/md5$ md5sum task4v1.o
67171d0e0c3e429d85c99adb3cc32142  task4v1.o
herbu@herbu-VirtualBox:~/md5$ gcc task4v1.c -o task4v1.o
herbu@herbu-VirtualBox:~/md5$ xxd task4v1.o | grep 4141
00003020: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003030: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003040: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003050: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003060: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003070: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003080: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003090: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030e0: 4141 4141 4141 4141 4743 433a 2028 5562  AAAAAAAAGCC: (Ub
```




```
herbu@herbu-VirtualBox:~/md5$ head -c 12352 task4v1.o > prefix
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p prefix -o task4v_out1.bin task4v_
out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'task4v_out1.bin' and 'task4v_out2.bin'
Using prefixfile: 'prefix'
Using initial value: ac2f39d6a5f3ec57de6f86d786ce1cfb

Generating first block: .
Generating second block: S00..........
Running time: 2.54668 s
```

```
herbu@herbu-VirtualBox:~/md5$ tail -c +12480 task4v1.o > suffix
herbu@herbu-VirtualBox:~/md5$ tail -c 128 task4v_out1.bin > p
herbu@herbu-VirtualBox:~/md5$ tail -c 128 task4v_out2.bin > q
```

```
herbu@herbu-VirtualBox:~/md5$ cat prefix p suffix > task4_1
herbu@herbu-VirtualBox:~/md5$ cat prefix q suffix > task4_2
herbu@herbu-VirtualBox:~/md5$ md5sum task4_1
69cf1684031983cdde760c80c1c91b72  task4_1
herbu@herbu-VirtualBox:~/md5$ md5sum task4_2
69cf1684031983cdde760c80c1c91b72  task4_2
herbu@herbu-VirtualBox:~/md5$ chmod +x task4_1
herbu@herbu-VirtualBox:~/md5$ ./task4_1
4141414141414141414141414141414141414141414141414141414141414141411b8c7ec2df551b1
245f54764f1b9062ac1482367f4df9635d676b1d42e36299dbb494c7e856ebfb48f2d6816246694
ad6f582f486e822d6ff83618aeb7b44df4f7f4be24f3073f09fe99b5495b5a23a23e5b6205dd9b7
14cd50725d2e7815ede71299f76c5a3a1ef71515c866fbce1c79e91fe2d96ecbd7de27c65174141
4141414141414141414141414141414141414141414141414141414141414141414141414141414141
```