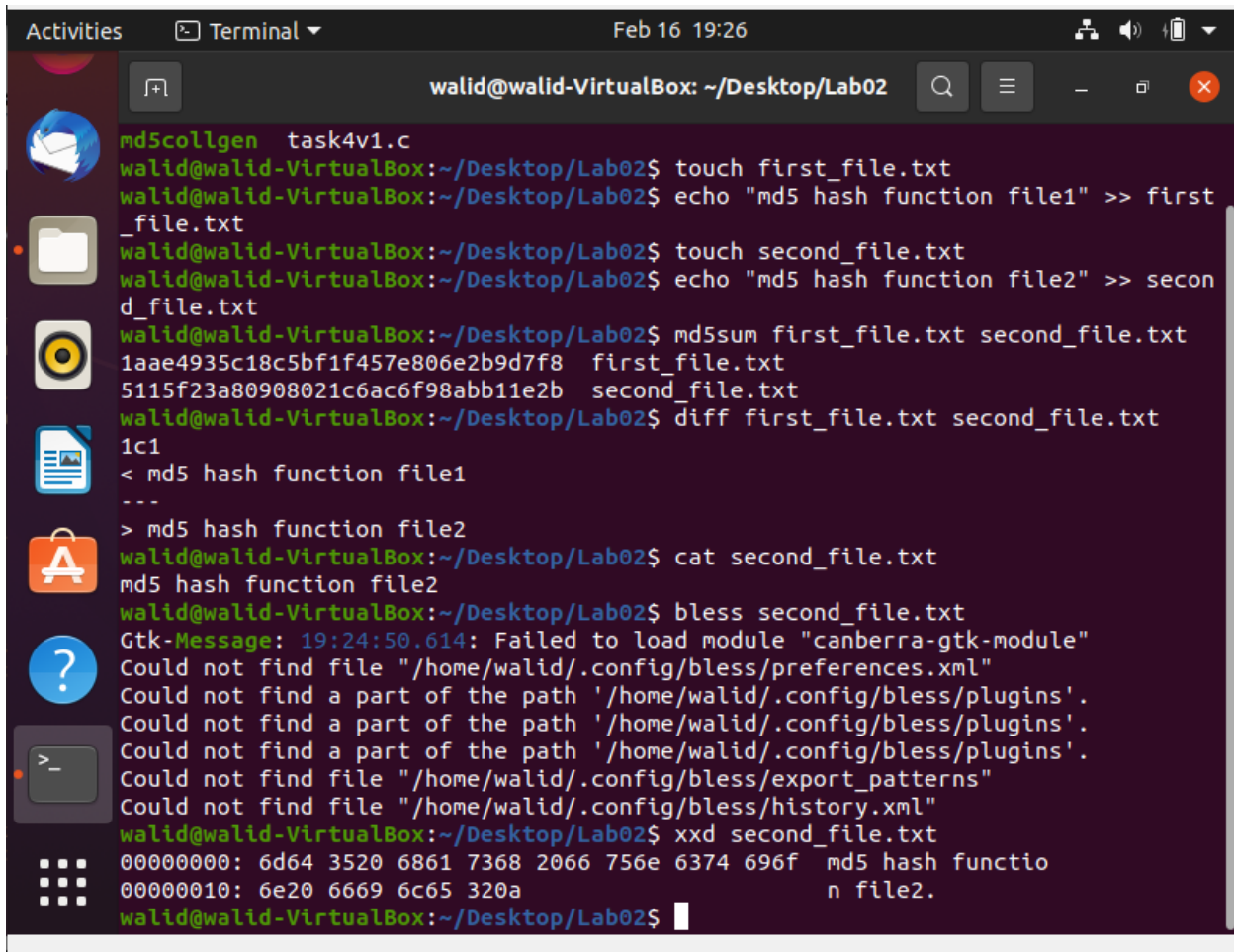


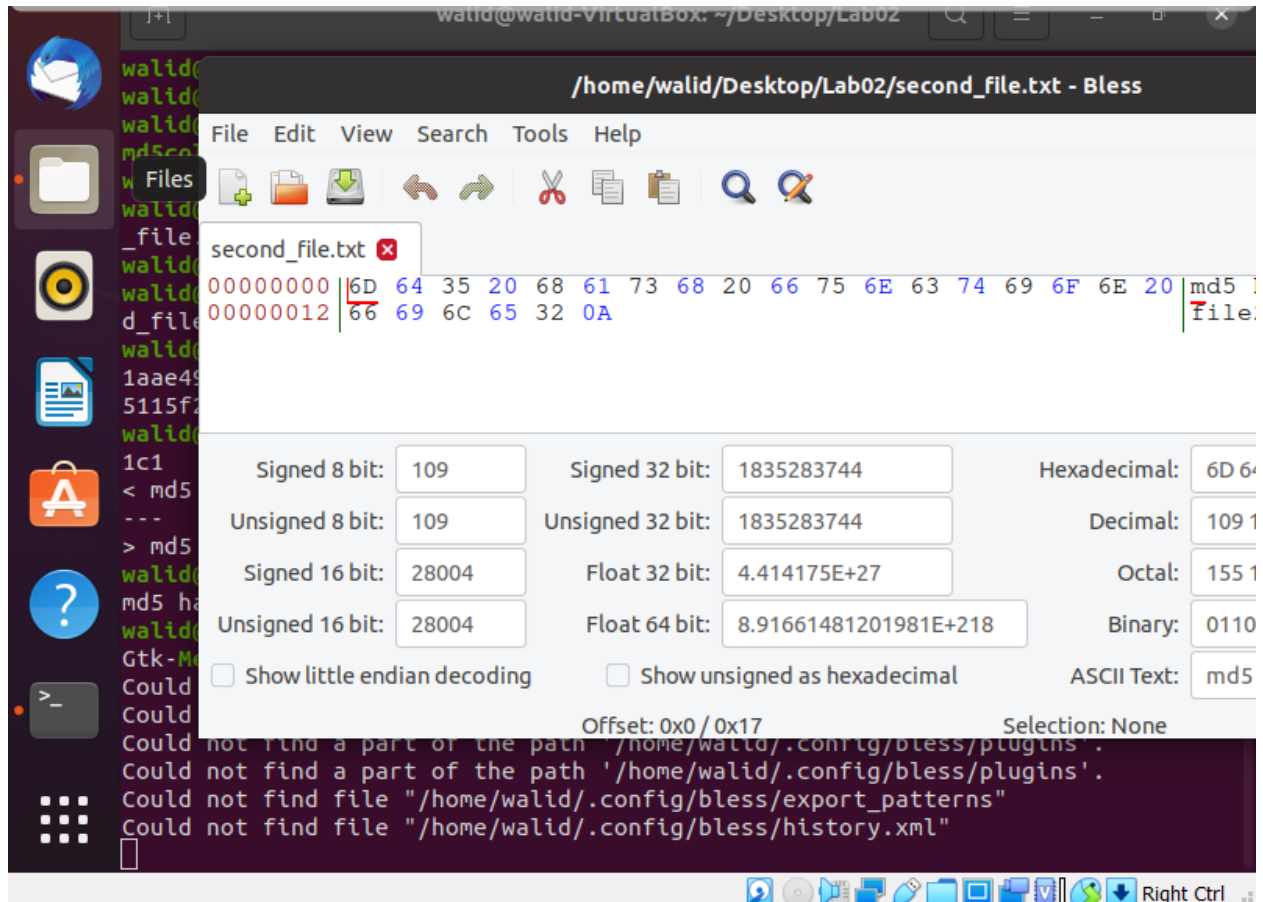
Lab #02 – Md5 collision
Lab Group 13
Kalid Ajibade (100660188)
Walid Ayub (100695612)
Zain Butt (100751676)
Konrad Herbus (100768380)

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



```
Activities Terminal Feb 16 19:26
walid@walid-VirtualBox: ~/Desktop/Lab02

md5collgen task4v1.c
walid@walid-VirtualBox:~/Desktop/Lab02$ touch first_file.txt
walid@walid-VirtualBox:~/Desktop/Lab02$ echo "md5 hash function file1" >> first_file.txt
walid@walid-VirtualBox:~/Desktop/Lab02$ touch second_file.txt
walid@walid-VirtualBox:~/Desktop/Lab02$ echo "md5 hash function file2" >> second_file.txt
walid@walid-VirtualBox:~/Desktop/Lab02$ md5sum first_file.txt second_file.txt
1aae4935c18c5bf1f457e806e2b9d7f8 first_file.txt
5115f23a80908021c6ac6f98abb11e2b second_file.txt
walid@walid-VirtualBox:~/Desktop/Lab02$ diff first_file.txt second_file.txt
1c1
< md5 hash function file1
---
> md5 hash function file2
walid@walid-VirtualBox:~/Desktop/Lab02$ cat second_file.txt
md5 hash function file2
walid@walid-VirtualBox:~/Desktop/Lab02$ bless second_file.txt
Gtk-Message: 19:24:50.614: Failed to load module "canberra-gtk-module"
Could not find file "/home/walid/.config/bleess/preferences.xml"
Could not find a part of the path '/home/walid/.config/bleess/plugins'.
Could not find a part of the path '/home/walid/.config/bleess/plugins'.
Could not find a part of the path '/home/walid/.config/bleess/plugins'.
Could not find file "/home/walid/.config/bleess/export_patterns"
Could not find file "/home/walid/.config/bleess/history.xml"
walid@walid-VirtualBox:~/Desktop/Lab02$ xxd second_file.txt
00000000: 6d64 3520 6861 7368 2066 756e 6374 696f md5 hash functio
00000010: 6e20 6669 6c65 320a                                n file2.
walid@walid-VirtualBox:~/Desktop/Lab02$
```



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$

```

```

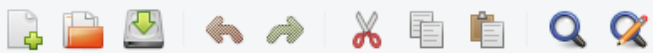
herbu@herbu-VirtualBox:~/md5$ touch prefix.txt
herbu@herbu-VirtualBox:~/md5$ echo "Lab2 md5collgen tool task2">> prefix.txt
herbu@herbu-VirtualBox:~/md5$ cat prefix.txt
Lab2 md5collgen tool task2
herbu@herbu-VirtualBox:~/md5$ ./md5collgen -p prefix.txt -o output1.bin output2
.bin
MD5 collision generator 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

```

/home/herbu/md5/output1.bin - Bless

File	Edit	View	Search	Tools	Help
					
output1.bin ✖					
00000000	4C	61	62	32	20 6D 64 35 63 6F 6C 6C 67 65 6E 20 74 6F
00000012	6F	6C	20	74	61 73 6B 32 0A 00 00 00 00 00 00 00 00 00 00
00000024	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000036	00	00	00	00	00 00 00 00 00 00 00 00 00 00 28 46 1E 52 34 7E 8B 10
00000048	44	0A	5F	4D	4F 42 55 BA 90 A0 EE 3D 4F 1B 2B 64 23 36

Lab2 md5collgen tool task2
.....
.....
D._MOBU..

Signed 8 bit:	76	Signed 32 bit:	1281450546	Hexadecimal:	4C 61 62 32
Unsigned 8 bit:	76	Unsigned 32 bit:	1281450546	Decimal:	076 097 098 0
Signed 16 bit:	19553	Float 32 bit:	5.908295E+07	Octal:	114 141 142 0
Unsigned 16 bit:	19553	Float 64 bit:	8.72947869525709E+59	Binary:	01001100 01
<input type="checkbox"/> Show little endian decoding		<input type="checkbox"/> Show unsigned as hexadecimal		ASCII Text: Lab2	
Offset: 0x0 / 0xbf				Selection: None	

/home/herbu/md5/output2.bin - Bless

File Edit View Search Tools Help

output2.bin

00000000	4C	61	62	32	20	6D	64	35	63	6F	6C	6C	67	65	6E	20	74	6F	Lab2 md5c
00000012	6F	6C	20	74	61	73	6B	32	0A	00	00	00	00	00	00	00	00	00	ol task2.
00000024	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000036	00	00	00	00	00	00	00	00	00	28	46	1E	52	34	7E	8B	10	
00000048	44	0A	5F	4D	4F	42	55	BA	90	A0	EE	BD	4F	1B	2B	64	23	36	D._MOBU..

Signed 8 bit: 76

Signed 32 bit: 1281450546

Hexadecimal: 4C 61 62 32

Unsigned 8 bit: 76

Unsigned 32 bit: 1281450546

Decimal: 076 097 098 0

Signed 16 bit: 19553

Float 32 bit: 5.908295E+07

Octal: 114 141 142 0

Unsigned 16 bit: 19553

Float 64 bit: 8.72947869525709E+59

Binary: 01001100 01

☐ Show little endian decoding
 ☐ Show unsigned as hexadecimal
 ASCII Text: Lab2

Offset: 0x0 / 0xbf Selection: None

```

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  ...=0.+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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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/X0.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/X0....
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
```

/home/herbu/md5/f1.txt - Bless

File Edit View Search Tools Help



F1.txt ✖

00000000	74	65	73	74	0A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	test.....
00000012	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000024	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000036	00	00	00	00	00	00	00	00	00	00	AC	5E	32	D7	17	16	3F	75	
00000048	E2	D3	5A	B6	D2	00	02	A3	F5	A9	B4	B6	A8	C9	44	18	FF	AD		..Z.....

Signed 8 bit:	116	Signed 32 bit:	1952805748	Hexadecimal:	74 65 73 74
Unsigned 8 bit:	116	Unsigned 32 bit:	1952805748	Decimal:	116 101 115
Signed 16 bit:	29797	Float 32 bit:	7.271592E+31	Octal:	164 145 163
Unsigned 16 bit:	29797	Float 64 bit:	4.91466258717606E+252	Binary:	01110100 01

☐ Show little endian decoding
 ☐ Show unsigned as hexadecimal
 ASCII Text: test

Offset: 0x0 / 0xc2 Selection: None

```
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

[illegible]

task4v1.o - GHex

File Edit View Windows Help

```

000000007F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00 00 ELF....
0000001003 00 3E 00 01 00 00 00 80 10 00 00 00 00 00 00 00 ..>.....
0000002040 00 00 00 00 00 00 00 A0 3A 00 00 00 00 00 00 00 @.....
0000003000 00 00 00 40 00 38 00 0D 00 40 00 1F 00 1E 00 00 ...@.8.
0000004006 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 00 .....(
0000005040 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 @.....(
00000060D8 02 00 00 00 00 00 00 D8 02 00 00 00 00 00 00 00 .....
0000007008 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 .....
0000008018 03 00 00 00 00 00 00 18 03 00 00 00 00 00 00 .....
0000009018 03 00 00 00 00 00 00 1C 00 00 00 00 00 00 00 .....

```

Signed 8 bit:	<input type="text" value="127"/>	Signed 32 bit:	<input type="text" value="1179403647"/>	Hexadecimal:	<input type="text" value="7F"/>
Unsigned 8 bit:	<input type="text" value="127"/>	Unsigned 32 bit:	<input type="text" value="1179403647"/>	Octal:	<input type="text" value="177"/>
Signed 16 bit:	<input type="text" value="17791"/>	Signed 64 bit:	<input type="text" value="1179403647"/>	Binary:	<input type="text" value="011"/>
Unsigned 16 bit:	<input type="text" value="17791"/>	Unsigned 64 bit:	<input type="text" value="1179403647"/>	Stream Length:	<input type="text" value="8"/>
Float 32 bit:	<input type="text" value="1.307337e+04"/>	Float 64 bit:	<input type="text" value="1.396152e-309"/>		

☒ Show little endian decoding ☐ Show unsigned and float as hexadecimal

Offset: 0x0

```

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

```

[illegible]