

## Colisión MD5

Para esta practica se uso el método de Peter Sellinger, el cual consiste en hacer un programa ejecutable con código “esquizofrenico” el cual incluye dos códigos con contenido diferente, y basándose en la función de MD5 se elige activar uno u otro código ya que la función de MD5 permite que los hashes arrojados sean iguales y nos da una ventana de 128 bytes en medio de los bloques elegidos para conformar el hash.

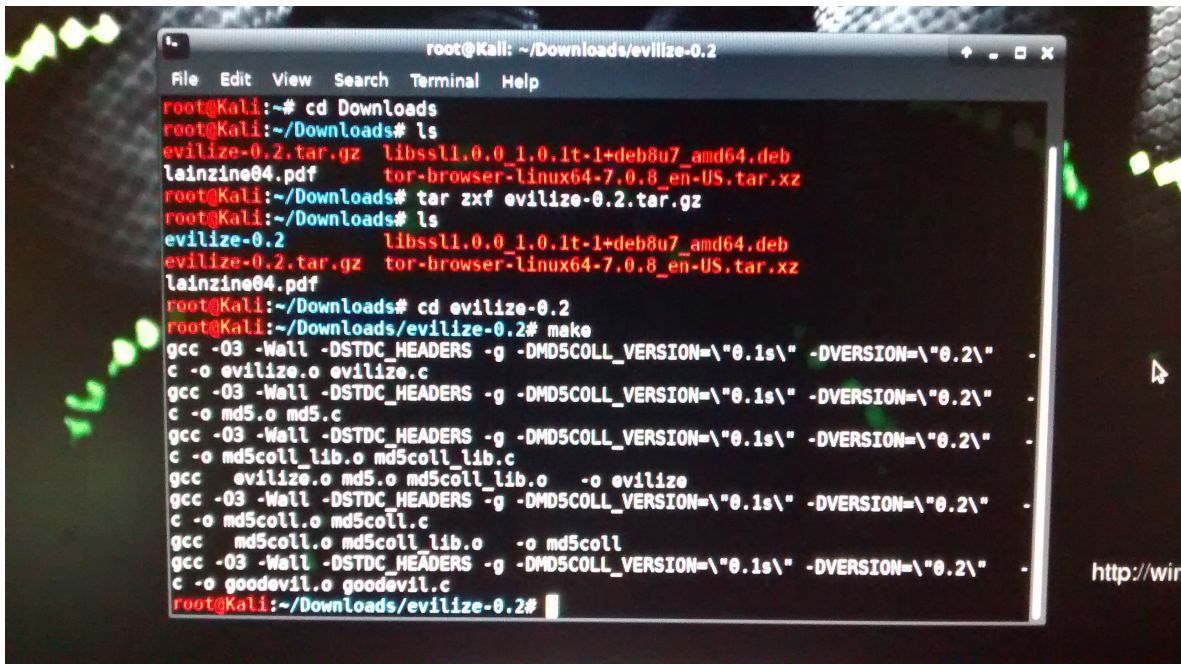
El programa que escribí es el siguiente:

```
#include <stdio.h>

main_good() {
    printf("hola, mundo!\n");
    return 0;
}

main_evil() {
    printf("ya te atrapo la vibora!!!\n");
    printf("Erasing hard drive...");
    printf("1Gb...");
    printf("2Gb...");
    printf(" caiste!\nbuendia.\n");
    return 0;
}
```

Utilice la herramienta *evilize* del mismo autor, la descomprimí y compile.

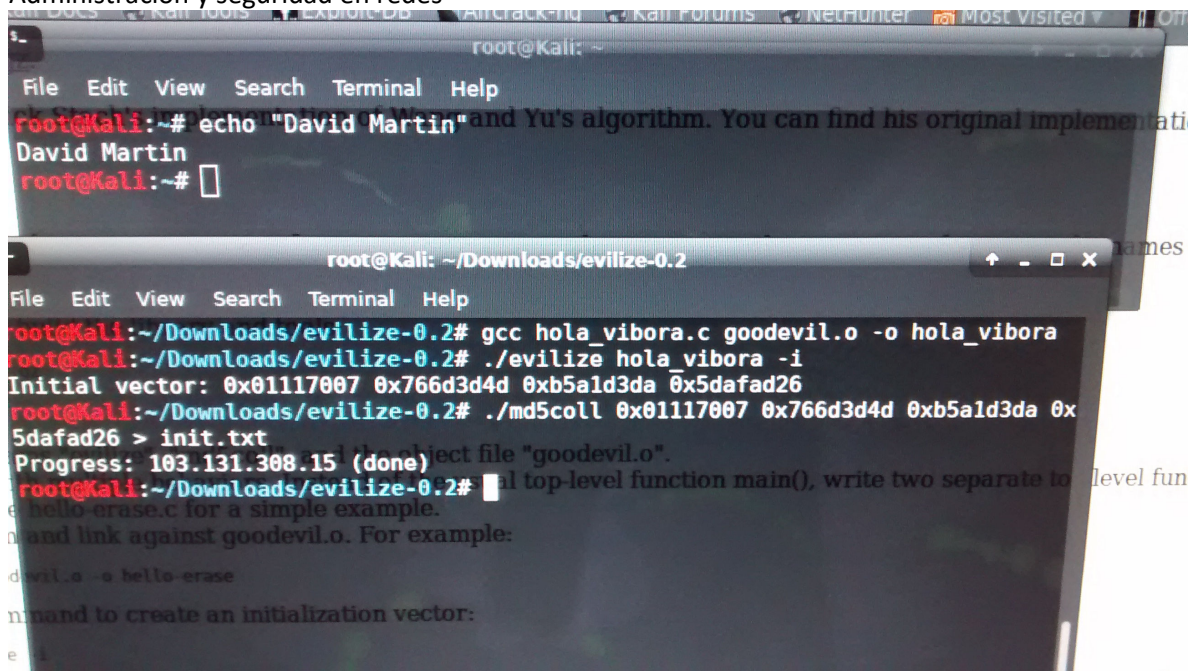


```

root@Kali: ~/Downloads/evilize-0.2
File Edit View Search Terminal Help
root@Kali:~# cd Downloads
root@Kali:~/Downloads# ls
evilize-0.2.tar.gz  libssl1.0.0_1.0.1t-1+deb8u7_amd64.deb
lainzine04.pdf     tor-browser-linux64-7.0.8_en-US.tar.xz
root@Kali:~/Downloads# tar xzf evilize-0.2.tar.gz
root@Kali:~/Downloads# ls
evilize-0.2  libssl1.0.0_1.0.1t-1+deb8u7_amd64.deb
evilize-0.2.tar.gz  tor-browser-linux64-7.0.8_en-US.tar.xz
lainzine04.pdf
root@Kali:~/Downloads# cd evilize-0.2
root@Kali:~/Downloads/evilize-0.2# make
gcc -O3 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -o evilize.o evilize.c
gcc -O3 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -o md5.o md5.c
gcc -O3 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -o md5coll_lib.o md5coll_lib.c
gcc evilize.o md5.o md5coll_lib.o -o evilize
gcc -O3 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -o md5coll.o md5coll.c
gcc md5coll.o md5coll_lib.o -o md5coll
gcc -O3 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -o goodevil.o goodevil.c
root@Kali:~/Downloads/evilize-0.2#

```

Compile mi código y lo uní al objeto *goodevil* para posteriormente lograr un vector de inicialización.



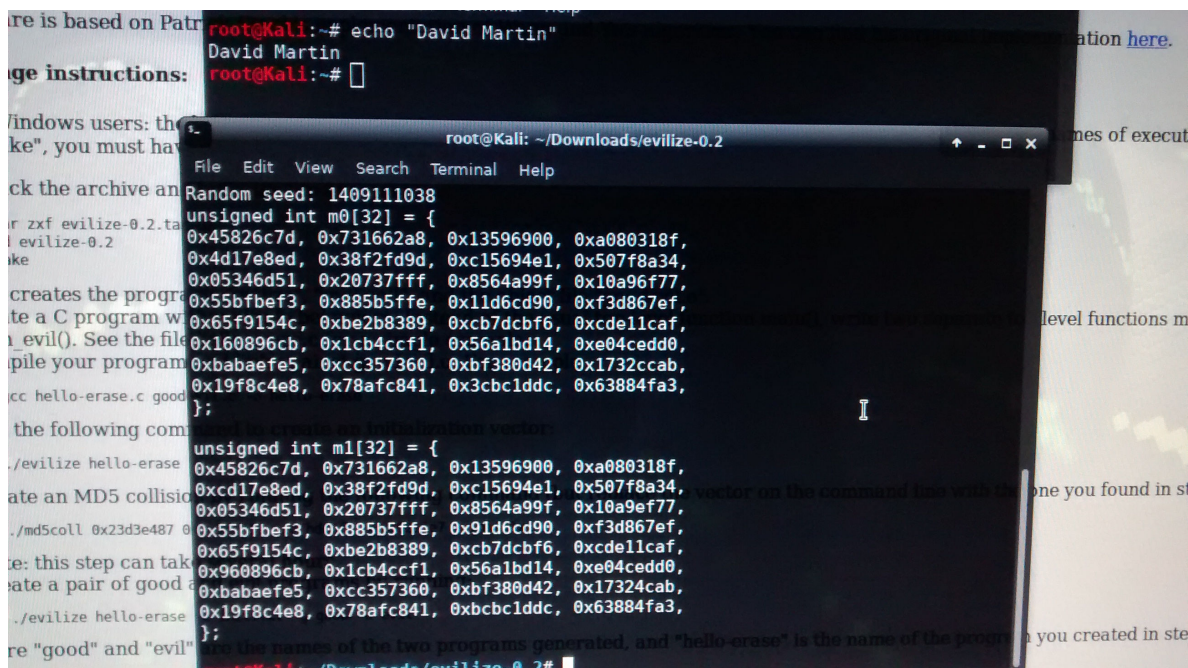
```

root@Kali: ~# echo "David Martin"
David Martin
root@Kali: ~#

root@Kali: ~/Downloads/evilize-0.2
File Edit View Search Terminal Help
root@Kali:~/Downloads/evilize-0.2# gcc hola_vibora.c goodevil.o -o hola_vibora
root@Kali:~/Downloads/evilize-0.2# ./evilize hola_vibora -i
Initial vector: 0x01117007 0x766d3d4d 0xb5a1d3da 0x5dafad26
root@Kali:~/Downloads/evilize-0.2# ./md5coll 0x01117007 0x766d3d4d 0xb5a1d3da 0x
5dafad26 > init.txt
Progress: 103.131.308.15 (done)
root@Kali:~/Downloads/evilize-0.2#

```

Se creo una colision de MD5



```

root@Kali: ~# echo "David Martin"
David Martin
root@Kali: ~#

root@Kali: ~/Downloads/evilize-0.2
File Edit View Search Terminal Help
Random seed: 1409111038
unsigned int m0[32] = {
0x45826c7d, 0x731662a8, 0x13596900, 0xa080318f,
0x4d17e8ed, 0x38f2fd9d, 0xc15694e1, 0x507f8a34,
0x05346d51, 0x20737fff, 0x8564a99f, 0x10a9ef77,
0x55bfbef3, 0x885b5ffe, 0x11d6cd90, 0xf3d867ef,
0x65f9154c, 0xbe2b8389, 0xcb7dcbf6, 0xcdellcaf,
0x160896cb, 0x1cb4ccf1, 0x56a1bd14, 0xe04cedd0,
0xbabae5, 0xcc357360, 0xbf380d42, 0x1732ccab,
0x19f8c4e8, 0x78afc841, 0x3cbc1ddc, 0x63884fa3,
};
unsigned int m1[32] = {
0x45826c7d, 0x731662a8, 0x13596900, 0xa080318f,
0xcd17e8ed, 0x38f2fd9d, 0xc15694e1, 0x507f8a34,
0x05346d51, 0x20737fff, 0x8564a99f, 0x10a9ef77,
0x55bfbef3, 0x885b5ffe, 0x91d6cd90, 0xf3d867ef,
0x65f9154c, 0xbe2b8389, 0xcb7dcbf6, 0xcdellcaf,
0x960896cb, 0x1cb4ccf1, 0x56a1bd14, 0xe04cedd0,
0xbabae5, 0xcc357360, 0xbf380d42, 0x1732cab,
0x19f8c4e8, 0x78afc841, 0x3cbc1ddc, 0x63884fa3,
};
root@Kali:~/Downloads/evilize-0.2#

```

Se generaron los dos programas con ayuda de evilize.



```

root@Kali:~# echo "David Martin"
David Martin
root@Kali:~#

root@Kali:~/Downloads/evilize-0.2# ./evilize hola_vibora -c init.txt -g p_hola -e p_vibora
Writing 'good' file p_hola.
Writing 'evil' file p_vibora.
root@Kali:~/Downloads/evilize-0.2# ls -l
total 508
-rw-rw---- 1 dm dm 178 Oct 11 2011 AUTHORS
-rw-rw---- 1 dm dm 172 Oct 11 2011 ChangeLog
-rw-rw---- 1 dm dm 17992 Oct 11 2011 COPYING
-rw-rw---- 1 dm dm 581 Oct 11 2011 crib.h
-rwxr-xr-x 1 root root 79872 Sep 30 17:21 evilize
-rw-rw---- 1 dm dm 11832 Oct 11 2011 evilize.c
-rw-rw---- 1 root root 54848 Sep 30 17:21 evilize.o
-rw-rw---- 1 dm dm 461 Oct 11 2011 goodevil.c
-rw-rw---- 1 root root 6128 Sep 30 17:21 goodevil.o
-rw-rw---- 1 dm dm 899 Oct 11 2011 hello-erase.c

```

Se otorgaron los permisos correspondientes de ejecución y se probó la funcionalidad, así mismo se generaron los dos hashes MD5..... con coincidencia exacta.

```

root@Kali:~/Downloads/evilize-0.2# ls -l p_*
-rw-r--r-- 1 root root 10560 Sep 30 19:14 p_hola
-rw-r--r-- 1 root root 10560 Sep 30 19:14 p_vibora
root@Kali:~/Downloads/evilize-0.2# chmod ugo+x p_*
root@Kali:~/Downloads/evilize-0.2# ls -l p_*
-rwxr-xr-x 1 root root 10560 Sep 30 19:14 p_hola
-rwxr-xr-x 1 root root 10560 Sep 30 19:14 p_vibora
root@Kali:~/Downloads/evilize-0.2# ./p_hola
hola, mundo!
root@Kali:~/Downloads/evilize-0.2# ./p_vibora
ya te atrapo la vibora!!!
Erasing hard drive...1Gb...2Gb... caiste!
buendia.
root@Kali:~/Downloads/evilize-0.2# md5sum p_hola
c659bed21b3476f7baf46ba5c24f6dd5 p_hola
root@Kali:~/Downloads/evilize-0.2# md5sum p_vibora
c659bed21b3476f7baf46ba5c24f6dd5 p_vibora
root@Kali:~/Downloads/evilize-0.2# echo "listo , David Martin"
listo , David Martin
root@Kali:~/Downloads/evilize-0.2#

```



Programa de Becas de Formación en Seguridad Informática  
Coordinación de Seguridad de la Información  
UNAM-CERT  
Administración y seguridad en redes

## **Bibliografía**

Selinger ,Peter. MD5 Collision. <https://www.mscs.dal.ca/~selinger/md5collision/>

Stevens, Dldier . Playing With Authenticode and MD5 Collisions.  
<https://blog.didierstevens.com/2009/01/17/playing-with-authenticode-and-md5-collisions/>