Programa filecarving

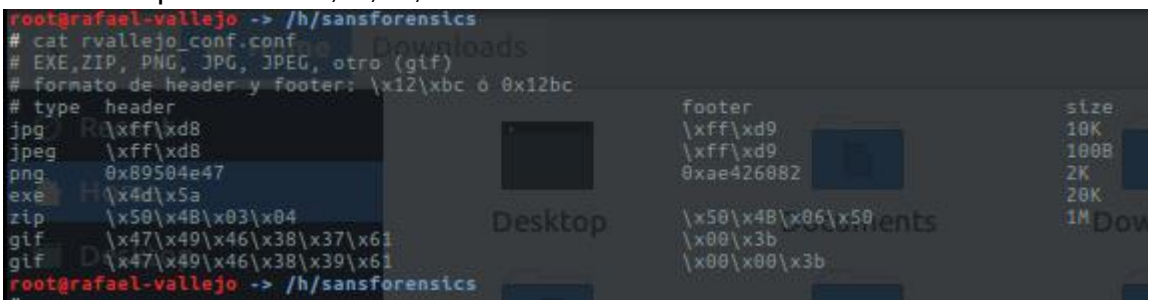
Para la prueba del script se utilizó la de captura proporcionada en clase (juego.pcap) los datos que fueron extraídos de ella (juego.raw).

Archivo de configuración:

Se especifica: tipo de archivos a recuperar, header, footer, tamaño

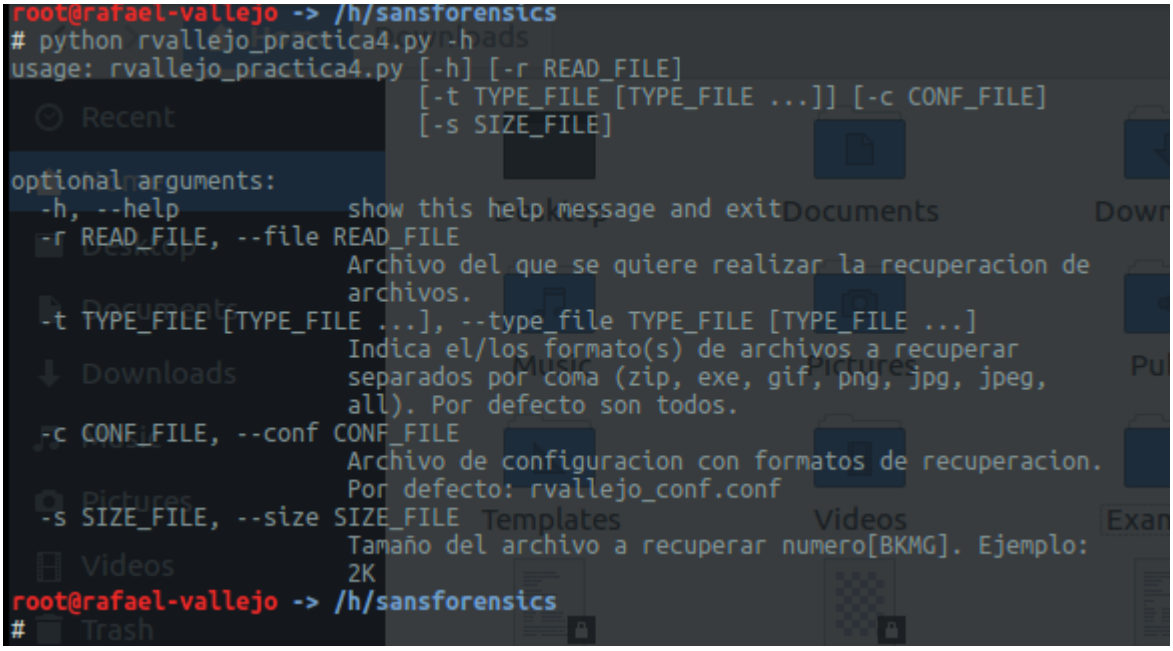
El formato de header y footer se especifica: \x12\xbc ó 0x12bc

El tamaño puede ser B, K, M, G



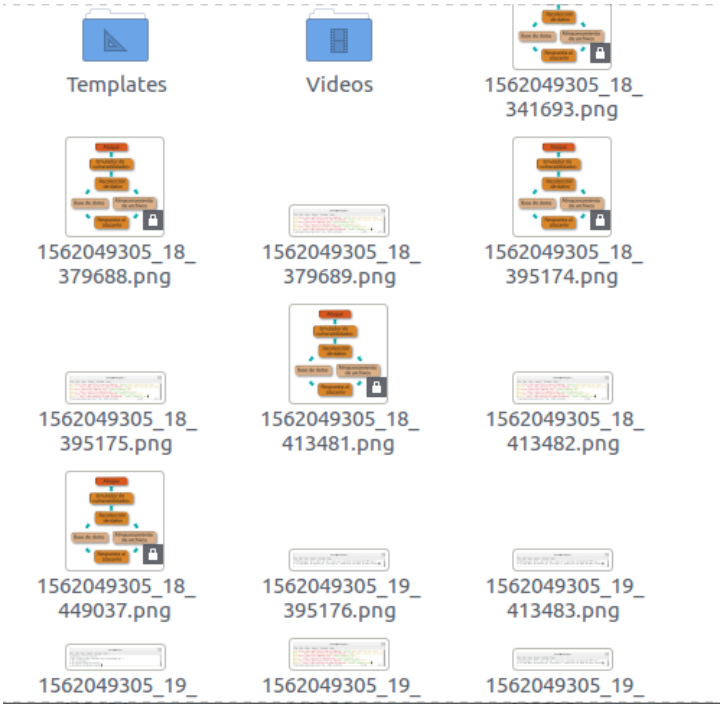
Ejecución del script desarrollado:

Las opciones del script son:



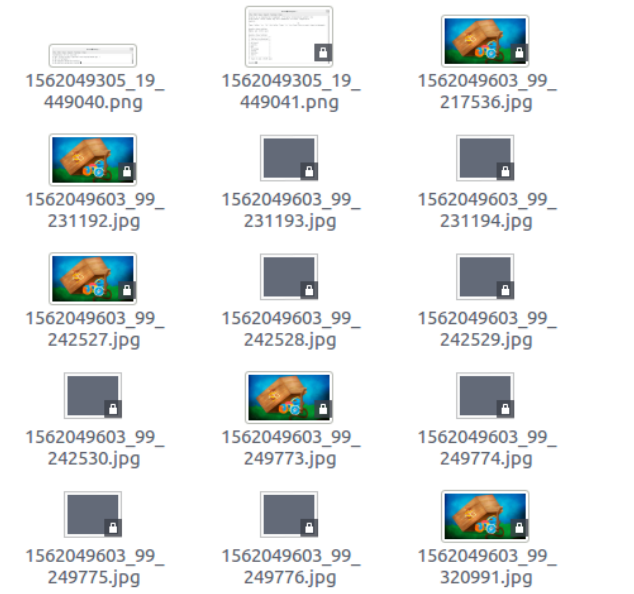
Se recuperan archivos png de juego.raw:

```
root@rafael-vallejo -> /h/sansforensics
# python rvallejo_practica4.py -c rvallejo_conf.conf -t png -r Downloads/juego.raw
Archivo recuperado: 1562049305_18_341693.png
Archivo recuperado: 1562049305_18_379688.png
Archivo recuperado: 1562049305_18_395174.png
Archivo recuperado: 1562049305_18_413481.png
Archivo recuperado: 1562049305_18_449037.png
Archivo recuperado: 1562049305_18_379689.png
Archivo recuperado: 1562049305_18_395175.png
Archivo recuperado: 1562049305_18_413482.png
Archivo recuperado: 1562049305_19_449038.png
Archivo recuperado: 1562049305_19_395176.png
Archivo recuperado: 1562049305_19_413483.png
Archivo recuperado: 1562049305_19_449039.png
Archivo recuperado: 1562049305_19_413484.png
Archivo recuperado: 1562049305_19_449040.png
Archivo recuperado: 1562049305_19_449041.png
root@rafael-vallejo -> /h/sansforensics
# ls -l *png
-rw-r--r-- 1 root root 123806 Jul  2 06:35 1562049305_18_341693.png
-rw-r--r-- 1 root root 161801 Jul  2 06:35 1562049305_18_379688.png
-rw-r--r-- 1 root root  37646 Jul  2 06:35 1562049305_18_379689.png
-rw-r--r-- 1 root root 177287 Jul  2 06:35 1562049305_18_395174.png
-rw-r--r-- 1 root root  53132 Jul  2 06:35 1562049305_18_395175.png
-rw-r--r-- 1 root root 195594 Jul  2 06:35 1562049305_18_413481.png
-rw-r--r-- 1 root root  71439 Jul  2 06:35 1562049305_18_413482.png
-rw-r--r-- 1 root root 231149 Jul  2 06:35 1562049305_18_449037.png
-rw-r--r-- 1 root root  15137 Jul  2 06:35 1562049305_19_395176.png
-rw-r--r-- 1 root root  33444 Jul  2 06:35 1562049305_19_413483.png
-rw-r--r-- 1 root root  17958 Jul  2 06:35 1562049305_19_413484.png
-rw-r--r-- 1 root root 106994 Jul  2 06:35 1562049305_19_449038.png
-rw-r--r-- 1 root root  68999 Jul  2 06:35 1562049305_19_449039.png
-rw-r--r-- 1 root root  53513 Jul  2 06:35 1562049305_19_449040.png
-rw-r--r-- 1 root root  35206 Jul  2 06:35 1562049305_19_449041.png
root@rafael-vallejo -> /h/sansforensics
#
```



Se recuperan archivos jpg de juego.raw:

```
root@rafael-vallejo -> /h/sansforensics
# python rvallejo_practica4.py -t jpg -r Downloads/juego.raw
Archivo recuperado: 1562049603_99_217536.jpg
Archivo recuperado: 1562049603_99_231192.jpg
Archivo recuperado: 1562049603_99_242527.jpg
Archivo recuperado: 1562049603_99_249773.jpg
Archivo recuperado: 1562049603_99_320991.jpg
Archivo recuperado: 1562049603_99_335428.jpg
Archivo recuperado: 1562049603_99_231193.jpg
Archivo recuperado: 1562049603_99_242528.jpg
Archivo recuperado: 1562049603_99_249774.jpg
Archivo recuperado: 1562049603_99_320992.jpg
Archivo recuperado: 1562049603_99_335429.jpg
Archivo recuperado: 1562049603_99_231194.jpg
Archivo recuperado: 1562049603_99_242529.jpg
Archivo recuperado: 1562049603_99_249775.jpg
Archivo recuperado: 1562049603_99_320993.jpg
Archivo recuperado: 1562049603_99_335430.jpg
Archivo recuperado: 1562049603_99_242530.jpg
Archivo recuperado: 1562049603_99_249776.jpg
Archivo recuperado: 1562049603_99_320994.jpg
Archivo recuperado: 1562049603_99_335431.jpg
Archivo recuperado: 1562049603_99_320995.jpg
Archivo recuperado: 1562049603_99_335432.jpg
root@rafael-vallejo -> /h/sansforensics
# ls -l *jpg
-rw-r--r-- 1 root root 155535 Jul  2 06:40 1562049603_99_217536.jpg
-rw-r--r-- 1 root root 169191 Jul  2 06:40 1562049603_99_231192.jpg
-rw-r--r-- 1 root root   2998 Jul  2 06:40 1562049603_99_231193.jpg
-rw-r--r-- 1 root root    961 Jul  2 06:40 1562049603_99_231194.jpg
-rw-r--r-- 1 root root 180526 Jul  2 06:40 1562049603_99_242527.jpg
-rw-r--r-- 1 root root  14333 Jul  2 06:40 1562049603_99_242528.jpg
-rw-r--r-- 1 root root  12296 Jul  2 06:40 1562049603_99_242529.jpg
-rw-r--r-- 1 root root    649 Jul  2 06:40 1562049603_99_242530.jpg
-rw-r--r-- 1 root root 187772 Jul  2 06:40 1562049603_99_249773.jpg
-rw-r--r-- 1 root root  21579 Jul  2 06:40 1562049603_99_249774.jpg
-rw-r--r-- 1 root root  19542 Jul  2 06:40 1562049603_99_249775.jpg
-rw-r--r-- 1 root root   7895 Jul  2 06:40 1562049603_99_249776.jpg
-rw-r--r-- 1 root root 258990 Jul  2 06:40 1562049603_99_320991.jpg
-rw-r--r-- 1 root root  92797 Jul  2 06:40 1562049603_99_320992.jpg
-rw-r--r-- 1 root root  90760 Jul  2 06:40 1562049603_99_320993.jpg
-rw-r--r-- 1 root root  79113 Jul  2 06:40 1562049603_99_320994.jpg
-rw-r--r-- 1 root root  58486 Jul  2 06:40 1562049603_99_320995.jpg
-rw-r--r-- 1 root root 273427 Jul  2 06:40 1562049603_99_335428.jpg
-rw-r--r-- 1 root root 107234 Jul  2 06:40 1562049603_99_335429.jpg
-rw-r--r-- 1 root root 105197 Jul  2 06:40 1562049603_99_335430.jpg
-rw-r--r-- 1 root root  93550 Jul  2 06:40 1562049603_99_335431.jpg
```



Se recuperan archivos exe de juego.pcap:

```
# python rvallejo_practica4.py -t exe -r Downloads/juego.pcap
20K
Archivo recuperado: 1562050788_71_105042.exe
Archivo recuperado: 1562050788_71_112948.exe
Archivo recuperado: 1562050788_71_114752.exe
Archivo recuperado: 1562050788_71_220228.exe
Archivo recuperado: 1562050788_71_230025.exe
Archivo recuperado: 1562050788_71_308101.exe
Archivo recuperado: 1562050788_71_324062.exe
Archivo recuperado: 1562050788_71_395376.exe
Archivo recuperado: 1562050788_71_395623.exe
Archivo recuperado: 1562050788_71_398166.exe
Archivo recuperado: 1562050788_71_403557.exe
Archivo recuperado: 1562050788_71_420754.exe
Archivo recuperado: 1562050788_71_428131.exe
Archivo recuperado: 1562050788_71_438729.exe
Archivo recuperado: 1562050788_72_478054.exe
Archivo recuperado: 1562050788_72_486278.exe
Archivo recuperado: 1562050788_72_506841.exe
Archivo recuperado: 1562050788_72_565737.exe
Archivo recuperado: 1562050788_72_658969.exe
Archivo recuperado: 1562050788_72_659696.exe
Archivo recuperado: 1562050788_72_660425.exe
Archivo recuperado: 1562050788_72_712943.exe
Archivo recuperado: 1562050788_72_736145.exe
Archivo recuperado: 1562050788_72_745464.exe
Archivo recuperado: 1562050788_72_748865.exe
Archivo recuperado: 1562050788_73_763136.exe
Archivo recuperado: 1562050788_73_765939.exe
Archivo recuperado: 1562050788_73_770661.exe
Archivo recuperado: 1562050788_73_771724.exe
Archivo recuperado: 1562050788_73_847795.exe
Archivo recuperado: 1562050788_73_851836.exe
Archivo recuperado: 1562050788_73_857460.exe
Archivo recuperado: 1562050788_73_875534.exe
Archivo recuperado: 1562050788_74_885897.exe
Archivo recuperado: 1562050788_74_909652.exe
Archivo recuperado: 1562050788_74_924257.exe
Archivo recuperado: 1562050788_74_934473.exe
Archivo recuperado: 1562050788_75_938593.exe
Archivo recuperado: 1562050788_75_941708.exe
Archivo recuperado: 1562050788_75_1025666.exe
Archivo recuperado: 1562050788_75_1030824.exe
Archivo recuperado: 1562050788_75_1031626.exe
```

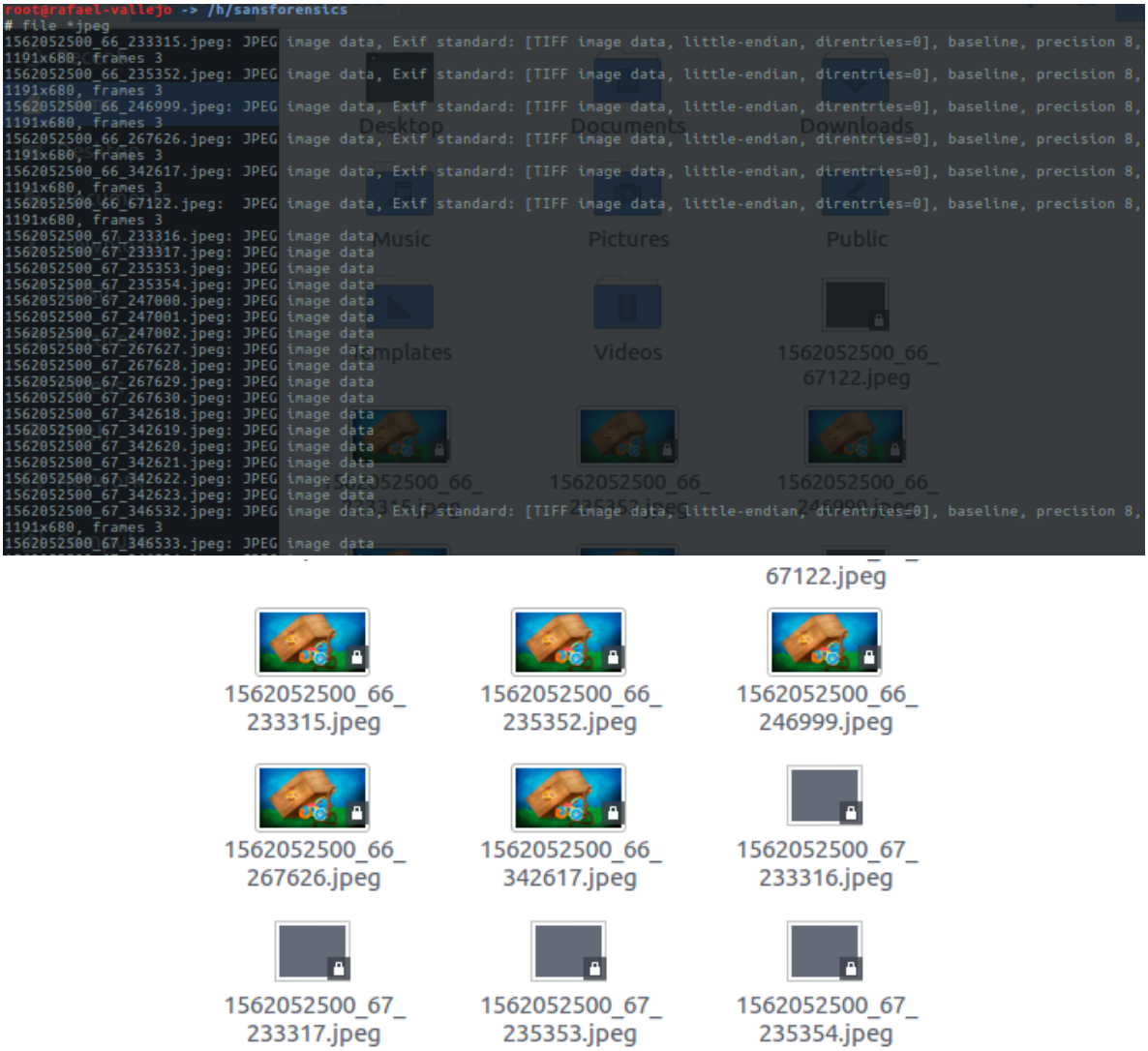
No todos los archivos exe recuperados son realmente ese tipo de archivos, sin embargo, al hacer un grep a los archivos recuperados, se observa que efectivamente fue posible recuperar algunos. Se tendrían que analizar para ver si realmente son útiles.

```
root@rafael-vallejo -> /h/sansforensics
# file *exe
1562050788_71_105042.exe:  data
1562050788_71_112948.exe:  data
1562050788_71_114752.exe:  data
1562050788_71_220228.exe:  data
1562050788_71_230025.exe:  data
1562050788_71_308101.exe:  data
1562050788_71_324062.exe:  data
1562050788_71_395376.exe:  data
1562050788_71_395623.exe:  data
1562050788_71_398166.exe:  data
1562050788_71_403557.exe:  data
1562050788_71_420754.exe:  data
1562050788_71_428131.exe:  data
1562050788_71_438729.exe:  data
1562050788_72_478054.exe:  data
1562050788_72_486278.exe:  data
1562050788_72_506841.exe:  data
1562050788_72_565737.exe:  data
```

```
root@rafael-vallejo -> /h/sansforensics
# file *exe | grep "MS-DOS"
1562050858_63_220232.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_63_230029.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_308105.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_324066.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_395380.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_395627.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_398170.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_403561.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_420758.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_428135.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_64_438733.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_65_478058.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_486282.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_506845.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_565741.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_658973.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_659700.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_66_660429.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_67_712947.exe:   MS-DOS executable, MZ for MS-DOS
1562050858_67_736149.exe:   MS-DOS executable, MZ for MS-DOS
```

Se recuperan archivos jpeg de tamaño de 5K del archivo juego.raw:

```
root@rafael-vallejo -> /h/sansforensics
# python rvallejo_practica4.py -t jpeg -r Downloads/juego.raw -s 5K
Archivo recuperado: 1562052500_66_67122.jpeg
Archivo recuperado: 1562052500_66_233315.jpeg
Archivo recuperado: 1562052500_66_235352.jpeg
Archivo recuperado: 1562052500_66_246999.jpeg
Archivo recuperado: 1562052500_66_267626.jpeg
Archivo recuperado: 1562052500_66_342617.jpeg
Archivo recuperado: 1562052500_67_346532.jpeg
Archivo recuperado: 1562052500_67_352136.jpeg
Archivo recuperado: 1562052500_67_233316.jpeg
Archivo recuperado: 1562052500_67_235353.jpeg
Archivo recuperado: 1562052500_67_247000.jpeg
Archivo recuperado: 1562052500_67_267627.jpeg
Archivo recuperado: 1562052500_67_342618.jpeg
Archivo recuperado: 1562052500_67_346533.jpeg
Archivo recuperado: 1562052500_67_352137.jpeg
Archivo recuperado: 1562052500_67_233317.jpeg
Archivo recuperado: 1562052500_67_235354.jpeg
Archivo recuperado: 1562052500_67_247001.jpeg
Archivo recuperado: 1562052500_67_267628.jpeg
Archivo recuperado: 1562052500_67_342619.jpeg
Archivo recuperado: 1562052500_67_346534.jpeg
Archivo recuperado: 1562052500_67_352138.jpeg
Archivo recuperado: 1562052500_67_247002.jpeg
Archivo recuperado: 1562052500_67_267629.jpeg
Archivo recuperado: 1562052500_67_342620.jpeg
Archivo recuperado: 1562052500_67_346535.jpeg
Archivo recuperado: 1562052500_67_352139.jpeg
Archivo recuperado: 1562052500_67_267630.jpeg
Archivo recuperado: 1562052500_67_342621.jpeg
Archivo recuperado: 1562052500_67_346536.jpeg
Archivo recuperado: 1562052500_67_352140.jpeg
Archivo recuperado: 1562052500_67_342622.jpeg
Archivo recuperado: 1562052500_67_346537.jpeg
Archivo recuperado: 1562052500_67_352141.jpeg
Archivo recuperado: 1562052500_67_342623.jpeg
Archivo recuperado: 1562052500_67_346538.jpeg
Archivo recuperado: 1562052500_67_352142.jpeg
Archivo recuperado: 1562052500_67_352143.jpeg
root@rafael-vallejo -> /h/sansforensics
```



Conclusión

La realización de este programa permitió trabajar con los datos en crudo de una captura, archivo para poder recuperar ciertos tipos de archivos, aunque no siempre que se recuperan son archivos útiles, pues muchas veces son archivos incompletos y se observó cuando al ejecutar el script desarrollado, se recuperaba una gran cantidad de archivos (exe, jpg) pero únicamente unos cuantos de ellos realmente pudieron recuperarse en su totalidad.

Para tener más precisión, es necesario hacer uso del archivo de configuración donde es posible agregar más tipos de archivos y de cambiar los header, footer y tamaños para lograr una mejor recuperación de archivos.

Estas herramientas de file carving son de gran utilidad para un análisis forense porque permiten la recuperación de archivos a partir de una captura de tráfico, de una imagen tipo raw, de archivos binarios, etcétera siendo necesario, en general, los valores utilizados en el archivo de configuración y que se vieron en clase.

Existen herramientas mucho más sofisticadas y esta práctica me dejó comprender mejor como es que un file carving trabaja, siendo la base de todas las herramientas existentes para ello.

Referencias

Martínez, A. (2015). File Carving. Recuperado el 01 de julio de 2019, de https://www.incibe-cert.es/blog/file-carving

(2019). FILE SIGNATURES TABLE. Recuperado el 01 de julio de 2019, de https://www.garykessler.net/library/file_sigs.html

re — Regular expression operations. Recuperado el 01 de julio de 2019, de https://docs.python.org/3/library/re.html