Programa filecarving

Se programó una herramienta que recupera archivos, para ello se tomo en cuenta el numero mágico

```
root@abraham-manzano -> ~/c/p/practica4
# python carver.py -h
Usage: carver.py [options]

Options:
  -h, --help            show this help message and exit
  -d DIRECTORY, --directory=DIRECTORY
                        Indica el directorio donde se guardaran los archivos
                        encontrados
  -f FILE, --file=FILE  Indica el archivo a analizar
  -c CONFIG, --config=CONFIG
                        Indica el archivo de configuracion
```

Las opciones son -d el cual indica el directorio donde se almacenarán los archivos encontrados

-f para indicar el archivo a analizar

-c para indicar el archivo de configuración

Las opciones -f y -d son obligatorias

Creando directorio para guardar archivos

```
root@abraham-manzano -> ~/c/p/practica4
# mkdir resultados
```

Archivo de configuración

```
#Archivo de configuracion
#Primero va el tipo de formato de archivo, luego el tamano en bytes y al final el n
umero magico
exe 640000   4D5A
zip 160000   504B0304
png 320000   504E47
jpg 1280000   FFD8
gif 640000   47494638
tar 2560000 7573746172
```

El archivo de prueba es juego.pcap (visto en clase)

```
root@abraham-manzano -> ~/c/p/practica4
# ls
carver.py  config.conf  juego.pcap  resultados
```

Funcionamiento de la herramienta

```
root@abraham-manzano -> ~/c/p/practica4
# python carver.py -d resultados/ -f juego.pcap

Archivo de configuracion
exe 640000   4D5A
zip 160000   504B0304
png 320000   504E47
jpg 1280000   FFD8
gif 640000   47494638
tar 2560000 7573746172

Archivo: juego.pcap
Directorio: resultados/
Configuraciòn: config.conf


Archivos tipo: exe
offset: 640000
Se creo el archivo llamado: "1562041902.49_0.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.49_1.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.49_2.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_3.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_4.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_5.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_6.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_7.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_8.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_9.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_10.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_11.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_12.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.5_13.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.51_14.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.51_15.exe" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.51_16.exe" en el directorio "resultados/"
```

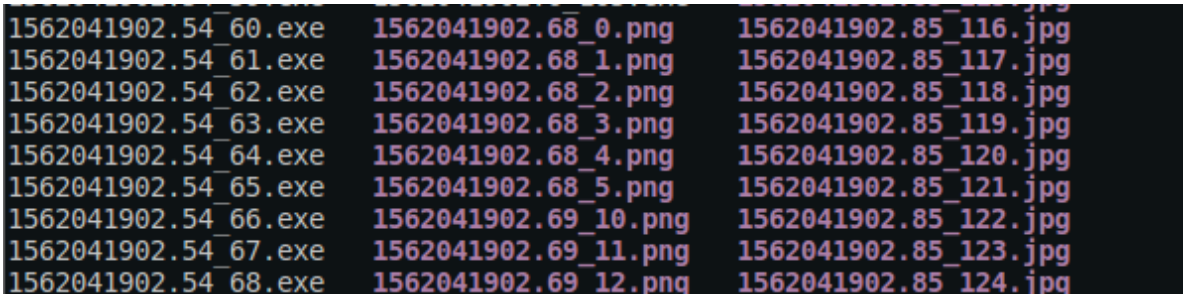
```
Se creo el archivo llamado: "1562041902.61_181.exe" en el directorio "resultados/"

Archivos tipo: png
offset: 320000
Se creo el archivo llamado: "1562041902.68_0.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.68_1.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.68_2.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.68_3.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.68_4.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.68_5.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.69_6.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.69_7.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.69_8.png" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.69_9.png" en el directorio "resultados/"
```

```
Se creo el archivo llamado: "1562041902.7_23.png" en el directorio "resultados/"

Archivos tipo: jpg
offset: 1280000
Se creo el archivo llamado: "1562041902.75_0.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.75_1.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.75_2.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.75_3.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.75_4.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_5.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_6.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_7.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_8.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_9.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_10.jpg" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.76_11.jpg" en el directorio "resultados/"
```

```
Se creo el archivo llamado: "1562041902.88_162.jpg" en el directorio "resultados/"

Archivos tipo: gif
offset: 640000
Se creo el archivo llamado: "1562041902.94_0.gif" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.94_1.gif" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.94_2.gif" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.95_3.gif" en el directorio "resultados/"
Se creo el archivo llamado: "1562041902.95_4.gif" en el directorio "resultados/"
```

Listando los archivos

```
root@abraham-manzano -> ~/c/p/practica4
# ls resultados/
1562041902.49_0.exe    1562041902.5_8.exe     1562041902.79_50.jpg
1562041902.49_1.exe    1562041902.59_130.exe  1562041902.79_51.jpg
1562041902.49_2.exe    1562041902.59_131.exe  1562041902.79_52.jpg
1562041902.5_10.exe    1562041902.59_132.exe  1562041902.81_65.jpg
1562041902.51_14.exe   1562041902.59_133.exe  1562041902.81_66.jpg
1562041902.51_15.exe   1562041902.59_134.exe  1562041902.81_67.jpg
1562041902.51_16.exe   1562041902.59_135.exe  1562041902.81_68.jpg
1562041902.51_17.exe   1562041902.59_136.exe  1562041902.81_69.jpg
1562041902.51_18.exe   1562041902.59_137.exe  1562041902.81_70.jpg
1562041902.51_19.exe   1562041902.59_138.exe  1562041902.81_71.jpg
1562041902.5_11.exe    1562041902.59_139.exe  1562041902.81_72.jpg
1562041902.51_20.exe   1562041902.59_140.exe  1562041902.81_73.jpg
1562041902.51_21.exe   1562041902.59_141.exe  1562041902.81_74.jpg
1562041902.51_22.exe   1562041902.59_142.exe  1562041902.82_75.jpg
1562041902.51_23.exe   1562041902.59_143.exe  1562041902.82_76.jpg
1562041902.51_24.exe   1562041902.59_144.exe  1562041902.82_77.jpg
1562041902.51_25.exe   1562041902.59_145.exe  1562041902.82_78.jpg
1562041902.51_26.exe   1562041902.59_146.exe  1562041902.82_79.jpg
```



Como se puede ver se obtienen algunos archivos, sin embargo, es poco probable que se restauren al cien por ciento.

Conclusiones

La práctica es muy útil para saber cómo se hacen este tipo de programas de manera general, obviamente hay herramientas mas potentes, sin embargo, este ejercicio nos ayuda a crear herramientas forenses de nuestra propia mano.

Referencias

https://docs.python.org/2/library/re.html

https://asecuritysite.com/forensics/magic

https://ubuntuforums.org/showthread.php?t=542809

https://github.com/sk8abraham/Analisis_software_malicioso/blob/master/practica2/cuarentena.py#L6