EPISODIO 1

200

Alguien ha denunciado a "El Flautista" por hacer actividades empresariales en una vivienda personal. Necesitamos encontrar a la persona en cuestión para convencerlo de que retire la denuncia o se nos caerá el pelo. El problema es que ha habido un apagón en la incubadora de Erlich y todos los discos duros han muerto menos el de Gilfoyle. En ellos estaban las credenciales de acceso (encriptadas) a la plataforma de la empresa y la única pista del denunciante. Debes conseguir las credenciales de alguno de los archivos de Gilfoyle para entrar y poder encontrar la dirección de la persona que ha montado todo este lío.

- Disco duro de Gilfoyle (escoged el enlace que mejor os venga):

http://www.mediafire.com/file/31pj2a5umpfm345/GILFOYLE-HELLDD.zip

https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhlv-JFLoNFVh8_dDvFCE-qjKuc

- Login: http://34.247.69.86/siliconvalley/episodio1/login.php

Info: La flag es el número de la casa en formato UAM{md5}

Nos descargamos el fichero zip y obtenemos un fichero raw. Después de examinarlo un poco vemos que es un volcado de memoria por lo que utilizaremos la fantástica utilidad volatility para el análisis forense.

root@kali:/media/sf_Downloads# volatility -f GILFOYLE-HELLDD.raw imageinfo

Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/media/sf_Downloads/GILFOYLE-HELLDD.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800029f00a0L

```
      Number of Processors : 1
    Image Type (Service Pack) : 1
              KPCR for CPU 0 : 0xfffff800029f1d00L
           KUSER_SHARED_DATA : 0xfffff78000000000L
         Image date and time : 2018-09-15 09:56:27 UTC+0000
    Image local date and time : 2018-09-15 11:56:27 +0200
```

Con esto obtenemos el perfil, por lo que ya podemos investigar que contiene.
Después de mirar bastante rato por los ficheros .. después de petar las contraseñas de Windows y pensar que el tema estaba en desencriptar las claves guardadas de firefox … no he dado con nada interesante, por lo que he seguido investigando más con volatility.

He encontrado dos métodos distintos para encontrar la contraseña, que son los siguientes:

Método 1:

root@kali:/media/sf_Downloads# volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP0x64 clipboard

```
Volatility Foundation Volatility Framework 2.6
Session    WindowStation Format                  Handle Object           Data
---------- ------------- ----------------- ----------------- ----------------
------------------------------------------------
         1 WinSta0       CF_UNICODETEXT              0x700e7 0xfffff900c01ce010
[448333920e12dc9fd9c5e8c...6166da47d52ffbf77b5d87]
         1 WinSta0       CF_TEXT               0x7400000000 ----------------
         1 WinSta0       CF_LOCALE                0x1200c5 0xfffff900c1d5a5a0
         1 WinSta0       0x0L                      0x0 ----------------
```

Parece interesante lo que hay copiado en el clipboard, por lo que busco directamente en el fichero raw a ver que hay:

root@kali:/media/sf_Downloads# strings GILFOYLE-HELLDD.raw | grep 448333920e12dc9fd9c5e8c

[448333920e12dc9fd9c5e8c30e6b1ea2]:[b3f894165d6166da47d52ffbf77b5d87]

Bien, parece un usuario y contraseña en md5, así que probamos a crackearlos en: https://crackstation.net/

Hash	Type	Result
448333920e12dc9fd9c5e8c30e6b1ea2	md5	Gilfoyle

b3f894165d6166da47d52ffbf77b5d87	md5	Satan

Vamos a http://34.247.69.86/siliconvalley/episodio1/login.php e introducimos los datos.

Método 2:

root@kali:~# volatility -f /media/sf_Downloads/GILFOYLE-HELLDD.raw --profile=Win7SP0x64 filescan > fitxers.txt

Vemos que hay un fichero .odt que se llama: info.odt

0x000000007fcabd50 1 1 RW-r-- \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt

Lo recuperamos:

root@kali:~# volatility -f /media/sf_Downloads/GILFOYLE-HELLDD.raw --profile=Win7SP0x64 dumpfiles -Q 0x000000007fcabd50 --name -D /media/sf_Downloads/uam/
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt

El aspecto es el siguiente:

Parece texto codificado en Base64, aunque hay una parte que no lo es debido a que tiene caracteres que no forman parte del alfabeto de codificación de Base64:

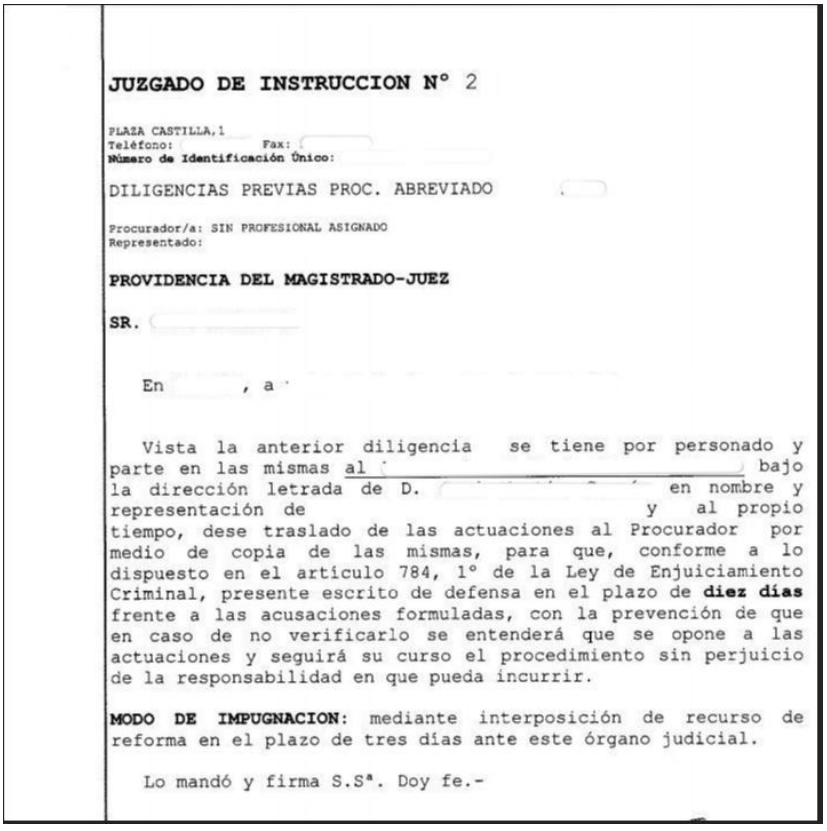
LjQKTGVnZW5kOiAoUykgPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0tLS0tLS0tLS
0tLS0tLS0tLS0tLS0tLQpSZWdpc3RyeTogXER1dmljZVxIYXJkZGlza1ZvbHVtZTFcV0lORE9X
U1xzeXN0ZW0zMlxjb25maWdcc3lzd[448333920e12dc9fd9c5e8c30e6b1ea2]:
[b3f894165d6166da47d52ffbf77b5d87]ZXQgKFMpCkxhc3QgdXBkYXR1ZDogMjAxMS0wNi0
wMyAwNDoyNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM6ClJF
R19TWiBEZXNjcmlwdGlvbiA6IChTKSBNUlhORVQKUkVHX1NalERpc3BsYXlOYW1lIDogK
FMpIE1SWE5FVApSRUdfRFdPUkQgRXJyb3JDb250cm9sIDogKFMpIDAKUkVHX1NalEdyb3

Parece un usuario:password en md5. * Vamos a método 1 para ver el resultado en claro.

Vamos a http://34.247.69.86/siliconvalley/episodio1/login.php e introducimos los datos.

Nos aparece otro link:
Denuncia recibida:
https://drive.google.com/open?id=10iguWjRmx3mB0Y4g9iRrJOIXZ1HlJ_zC

Allí nos descargamos una imagen jpeg:



JUZGADO DE INSTRUCCION Nº 2

PLAZA CASTILLA,1
Teléfono: Fax:
Número de Identificación Único:

DILIGENCIAS PREVIAS PROC. ABREVIADO

Procurador/a: SIN PROFESIONAL ASIGNADO
Representado:

PROVIDENCIA DEL MAGISTRADO-JUEZ

SR.

En , a

Vista la anterior diligencia se tiene por personado y parte en las mismas al bajo la dirección letrada de D. en nombre y representación de y al propio tiempo, dese traslado de las actuaciones al Procurador por medio de copia de las mismas, para que, conforme a lo dispuesto en el artículo 784, 1º de la Ley de Enjuiciamiento Criminal, presente escrito de defensa en el plazo de **diez días** frente a las acusaciones formuladas, con la prevención de que en caso de no verificarlo se entenderá que se opone a las actuaciones y seguirá su curso el procedimiento sin perjuicio de la responsabilidad en que pueda incurrir.

MODO DE IMPUGNACION: mediante interposición de recurso de reforma en el plazo de tres días ante este órgano judicial.

Lo mandó y firma S.Sª. Doy fe.-

Miramos qué metadatos tiene la imagen:

```
root@kali:/media/sf_Downloads# exiftool denuncia.jpeg
ExifTool Version Number         : 11.10
File Name                       : denuncia.jpeg
Directory                       : .
File Size                       : 191 kB
File Modification Date/Time     : 2018:09:15 22:09:01+02:00
File Access Date/Time           : 2018:09:15 22:09:01+02:00
File Inode Change Date/Time     : 2018:09:15 22:09:01+02:00
File Permissions                : rwxrwx---
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Processing Software             : Windows Photo Editor 10.0.10011.16384
Orientation                     : Horizontal (normal)
Software                        : Windows Photo Editor 10.0.10011.16384
Modify Date                     : 2018:09:15 22:08:57
Padding                         : (Binary data 2060 bytes, use -b option to extract)
XMP Toolkit                     : Image::ExifTool 11.10
Location                        : 37.436712, -122.137837
Creator Tool                    : Windows Photo Editor 10.0.10011.16384
```

Obtenemos unas coordenadas, fijémonos en Location.
Aquí he de decir que he perdido mucho tiempo, ya que ya había visto esas coordenadas, pero no he caído en que la serie se desarrolla en Silicon Valley y al darme las coordenadas fuera de España lo había descartado ¬_¬’
He estado haciendo mil pruebas de stego a la imagen … jugando con perfiles ICC ya que tanto con exiftool como con binwalk había alguna pista que apuntaba a algo de eso … Al final, he ido a mirar bien las coordenadas (37.436712, -122.137837) en google maps:

MD5 hash for 2126 is : **3b92d18aa7a6176dd37d372bc2f1eb71**

DarkEagle