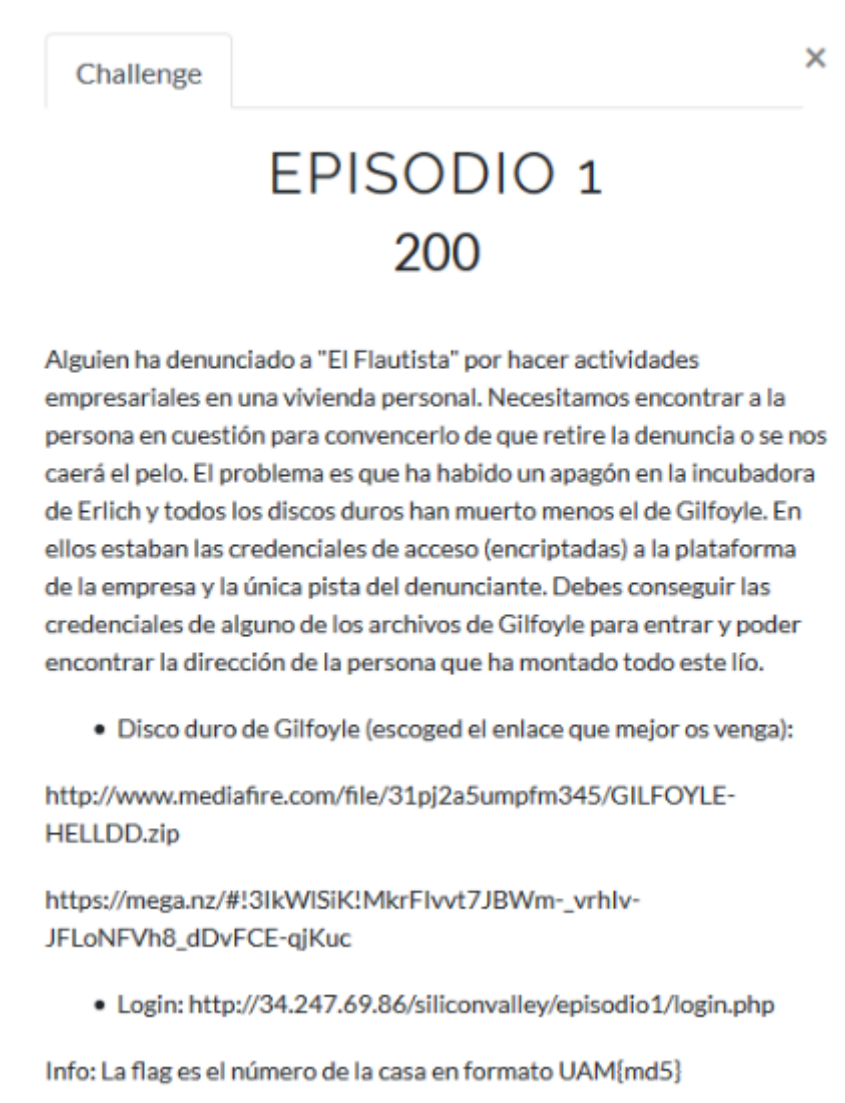
# Una al Mes (Silicon Valley - Episodio 1)

@percu

18/09/18

## Contenido

# MISIÓN



Challenge

## 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/#!3IkWISiK!MkrFIvvt7JBWm-_vrhIv-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}

# RESOLUCIÓN

## PARTE 1 – FORENSE

El primer paso es descargarnos el fichero de una de las url's suministradas. Dicho fichero es un comprimido .zip que contiene otro con extensión '.raw'.

Como tenemos que encontrar las credenciales encriptadas del disco de Gilfoyle lo primero que se nos ocurre es que ese fichero sea un dump de su disco duro, pero con el comando '*file'* no nos arroja ningún resultado.

Comprobamos entonces que es un dump de memoria:

```
>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 (/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
```

Pues empecemos. Dump de memoria de un sistema Windows 7 de 64 bits. Analizamos procesos activos en el momento del dump de memoria *'pstree'*:

```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa80018ac040:System                             4      0     80    557 2018-09-15 09:47:47 UTC+0000
. 0xfffffa8002101040:smss.exe                        248      4      2     29 2018-09-15 09:47:47 UTC+0000
 0xfffffa80028c6b30:csrss.exe                        324    316      9    411 2018-09-15 09:47:51 UTC+0000
 0xfffffa80028ed060:wininit.exe                      380    316      3     75 2018-09-15 09:47:51 UTC+0000
. 0xfffffa80028f1b30:services.exe                    468    380      8    193 2018-09-15 09:47:52 UTC+0000
.. 0xfffffa8002e8a9e0:SearchIndexer.                1160    468     11    611 2018-09-15 09:48:14 UTC+0000
... 0xfffffa8001d37060:SearchFilterHo               3852   1160      5     24 2018-09-15 09:57:22 UTC+0000
... 0xfffffa80019de960:SearchProtocol               3824   1160      7    769 2018-09-15 09:57:22 UTC+0000
.. 0xfffffa8002d42b30:taskhost.exe                  1804    468     10    255 2018-09-15 09:48:05 UTC+0000
.. 0xfffffa8002a00b30:svchost.exe                    784    468     22    573 2018-09-15 09:47:56 UTC+0000
... 0xfffffa8002fc9b30:audiodg.exe                  1856    784      5    127 2018-09-15 09:53:34 UTC+0000
.. 0xfffffa8002abeb30:svchost.exe                    532    468     14    379 2018-09-15 09:47:58 UTC+0000
.. 0xfffffa8002be15f0:svchost.exe                   1324    468     19    273 2018-09-15 09:48:01 UTC+0000
.. 0xfffffa8002b59b30:svchost.exe                   1204    468     19    300 2018-09-15 09:48:01 UTC+0000
.. 0xfffffa80029c2420:svchost.exe                    696    468      7    285 2018-09-15 09:47:55 UTC+0000
.. 0xfffffa8002a6e060:svchost.exe                   1012    468      5    110 2018-09-15 09:47:57 UTC+0000
.. 0xfffffa8002a1bb30:svchost.exe                    828    468     25    491 2018-09-15 09:47:56 UTC+0000
... 0xfffffa8002d71300:dwm.exe                      1864    828      3     71 2018-09-15 09:48:05 UTC+0000
.. 0xfffffa8002f7fb30:svchost.exe                   2236    468      8    346 2018-09-15 09:48:17 UTC+0000
.. 0xfffffa8002ec4b30:wmpnetwk.exe                  2008    468     13    415 2018-09-15 09:48:16 UTC+0000
.. 0xfffffa8002f619e0:svchost.exe                   2404    468     13    326 2018-09-15 09:50:03 UTC+0000
.. 0xfffffa8001f76720:spoolsv.exe                   1120    468     13    269 2018-09-15 09:48:00 UTC+0000
.. 0xfffffa800298e910:svchost.exe                    572    468     10    349 2018-09-15 09:47:54 UTC+0000
... 0xfffffa8001d67b30:WmiPrvSE.exe                 2328    572      6    120 2018-09-15 09:56:02 UTC+0000
... 0xfffffa8001d598b0:explorer.exe                 2692    572     16    507 2018-09-15 09:55:59 UTC+0000
.... 0xfffffa8001d2b060:DumpIt.exe                  3596   2692      5     46 2018-09-15 09:56:18 UTC+0000
... 0xfffffa8003029b30:WmiPrvSE.exe                 2516    572      7    113 2018-09-15 09:48:23 UTC+0000
.. 0xfffffa8002a286c0:svchost.exe                    876    468     31    873 2018-09-15 09:47:56 UTC+0000
.. 0xfffffa80029a6060:VBoxService.ex                 632    468     12    116 2018-09-15 09:47:55 UTC+0000
.. 0xfffffa8002a22b30:svchost.exe                    852    468     18    467 2018-09-15 09:47:56 UTC+0000
. 0xfffffa8002930430:lsass.exe                       476    380      8    718 2018-09-15 09:47:53 UTC+0000
. 0xfffffa800194bb30:lsm.exe                         484    380     10    144 2018-09-15 09:47:53 UTC+0000
 0xfffffa80019289e0:explorer.exe                    1900   1852     34    922 2018-09-15 09:48:06 UTC+0000
. 0xfffffa8002d24b30:soffice.exe                    1756   1900      1     66 2018-09-15 09:48:13 UTC+0000
.. 0xfffffa8002fc7b30:soffice.bin                   2340   1756     11    464 2018-09-15 09:48:18 UTC+0000
. 0xfffffa8002e3b290:VBoxTray.exe                   1376   1900     14    159 2018-09-15 09:48:08 UTC+0000
 0xfffffa80028ee5e0:winlogon.exe                     408    364      5    116 2018-09-15 09:47:52 UTC+0000
 0xfffffa80028df9e0:csrss.exe                        372    364      9    342 2018-09-15 09:47:51 UTC+0000
. 0xfffffa8001e1b060:conhost.exe                    3608    372      2     51 2018-09-15 09:56:18 UTC+0000
 0xfffffa8001d61b30:firefox.exe                      956   3052      0 ------ 2018-09-15 09:55:59 UTC+0000
```

Con un vistazo rápido nos quedamos que hay en ejecución un Firefox y un Open Office.

Probamos con los procesos terminados *'psscan'*:

```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000007e629b30 WmiPrvSE.exe       2516    572 0x000000000b044000 2018-09-15 09:48:23 UTC+0000
0x000000007e83b290 VBoxTray.exe       1376   1900 0x0000000013a49000 2018-09-15 09:48:08 UTC+0000
0x000000007e88a9e0 SearchIndexer.     1160    468 0x0000000011d76000 2018-09-15 09:48:14 UTC+0000
0x000000007e8c4b30 wmpnetwk.exe       2008    468 0x000000001057c000 2018-09-15 09:48:16 UTC+0000
0x000000007e9619e0 svchost.exe        2404    468 0x000000006e01f000 2018-09-15 09:50:03 UTC+0000
0x000000007e97fb30 svchost.exe        2236    468 0x000000000e301000 2018-09-15 09:48:17 UTC+0000
0x000000007e9c7b30 soffice.bin        2340   1756 0x000000000e04a000 2018-09-15 09:48:18 UTC+0000
0x000000007e9c9b30 audiodg.exe        1856    784 0x00000000bdd7000 2018-09-15 09:53:34 UTC+0000
0x000000007eb24b30 soffice.exe        1756   1900 0x0000000011faf000 2018-09-15 09:48:13 UTC+0000
0x000000007eb42b30 taskhost.exe       1804    468 0x0000000015f8c000 2018-09-15 09:48:05 UTC+0000
0x000000007eb71300 dwm.exe            1864    828 0x0000000015ca4000 2018-09-15 09:48:05 UTC+0000
0x000000007ec00b30 svchost.exe         784    468 0x0000000022373000 2018-09-15 09:47:56 UTC+0000
0x000000007ec1bb30 svchost.exe         828    468 0x0000000022183000 2018-09-15 09:47:56 UTC+0000
0x000000007ec22b30 svchost.exe         852    468 0x0000000021f8b000 2018-09-15 09:47:56 UTC+0000
0x000000007ec286c0 svchost.exe         876    468 0x0000000021d16000 2018-09-15 09:47:56 UTC+0000
0x000000007ec6e060 svchost.exe        1012    468 0x00000000209a2000 2018-09-15 09:47:57 UTC+0000
0x000000007ecbeb30 svchost.exe         532    468 0x000000001ed28000 2018-09-15 09:47:58 UTC+0000
0x000000007ed59b30 svchost.exe        1204    468 0x000000001a32b000 2018-09-15 09:48:01 UTC+0000
0x000000007ede15f0 svchost.exe        1324    468 0x0000000019b88000 2018-09-15 09:48:01 UTC+0000
0x000000007eec6b30 csrss.exe           324    316 0x0000000025182000 2018-09-15 09:47:51 UTC+0000
0x000000007eedf9e0 csrss.exe           372    364 0x000000024e11000 2018-09-15 09:47:51 UTC+0000
0x000000007eeed060 wininit.exe         380    316 0x0000000024b88000 2018-09-15 09:47:51 UTC+0000
0x000000007eeee5e0 winlogon.exe        408    364 0x0000000024a17000 2018-09-15 09:47:52 UTC+0000
0x000000007eef1b30 services.exe        468    380 0x000000023e0f000 2018-09-15 09:47:52 UTC+0000
0x000000007ef30430 lsass.exe           476    380 0x0000000023eb0000 2018-09-15 09:47:53 UTC+0000
0x000000007ef8e910 svchost.exe         572    468 0x0000000002337b000 2018-09-15 09:47:54 UTC+0000
0x000000007efa6060 VBoxService.ex      632    468 0x0000000022c9b000 2018-09-15 09:47:55 UTC+0000
0x000000007efc2420 svchost.exe         696    468 0x0000000022a49000 2018-09-15 09:47:55 UTC+0000
0x000000007f701040 smss.exe            248      4 0x000000002c49a000 2018-09-15 09:47:47 UTC+0000
0x000000007f81b060 conhost.exe        3608    372 0x0000000016f48000 2018-09-15 09:56:18 UTC+0000
0x000000007f976720 spoolsv.exe        1120    468 0x000000001b63e000 2018-09-15 09:48:00 UTC+0000
0x000000007fb2b060 DumpIt.exe         3596   2692 0x0000000016cc3000 2018-09-15 09:56:18 UTC+0000
0x000000007fb37060 SearchFilterHo     3852   1160 0x0000000053b1d000 2018-09-15 09:57:22 UTC+0000
0x000000007fb598b0 explorer.exe       2692    572 0x000000001ab61000 2018-09-15 09:55:59 UTC+0000
0x000000007fb61b30 firefox.exe         956   3052 0x0000000016790000 2018-09-15 09:55:59 UTC+0000   2018-09-15 09:56:08 UTC+0000
0x000000007fb67600 firefox.exe        1684    956 0x0000000075de1000 2018-09-15 09:56:02 UTC+0000   2018-09-15 09:56:08 UTC+0000
0x000000007fb67b30 WmiPrvSE.exe       2328    572 0x0000000076bcb000 2018-09-15 09:56:02 UTC+0000
0x000000007fbca6c0 pingsender.exe     3212    956 0x0000000060069a000 2018-09-15 09:56:08 UTC+0000   2018-09-15 09:56:09 UTC+0000
0x000000007fe5b960 SearchProtocol     3824   1160 0x0000000059d16000 2018-09-15 09:57:22 UTC+0000
0x000000007fea59e0 explorer.exe       1900   1852 0x0000000073280000 2018-09-15 09:48:06 UTC+0000
0x000000007fec8b30 lsm.exe             484    380 0x0000000023f36000 2018-09-15 09:47:53 UTC+0000
0x000000007ff29040 System                4      0 0x0000000000187000 2018-09-15 09:47:47 UTC+0000
```

Solamente observamos otro proceso Firefox…

Lo primero que se nos ocurre es intentar mirar las cookies del Firefox por si Gilfoyle esta logueado y apreciamos el usuario en ella. Utilizamos el plugin firefoxhistory.py para volatility de superponible per no encontramos ninguna cookie que nos indique algo. Tampoco vemos en el historial del Firefox nada apreciable:

```
>volatility --plugins=./volatility-plugins-master/ -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 firefoxcookies
Volatility Foundation Volatility Framework 2.6
Row ID Base Domain                App Id InBrowserElement Name                 Value                          Host
                       Expiry              Last Accessed             Creation Time             Secure HttpOnly
------ ---------------------------- ------ --------------- -------------------- ------------------------------ ------------------------------
---------------------- ------------------- ------------------- ------------------- ------ --------
    15                          n/a    n/a               everesttec             h.neteverest_g_v2g_surferid      ~Wfd_agAAAH206mw               -
                   1994-09-01 06:36:21  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    15                          n/a    n/a               eve                    resttech.netgglckCAESEEvWT0      _eFsjhqP78oBZqYI               Q
                   1994-09-01 06:36:21  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    16                          n/a    n/a               rlcd                   n.comrtn1-zIaPV...JifX9wJPrgfrVs IzID2MQAK7                     n
                   1994-09-11 02:33:07  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    16                          n/a    n/a               ads                    rvr.orgTDCPMCAE...Y1EAU4AVoIbGl2 ZXJhbXBgAg.                    .
                   1994-08-29 04:30:43  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    15                          n/a    n/a               ad                     srvr.orgTDID9d7...c61-4714-ba71- 80f3265eb67                    1
                   1994-08-29 04:30:43  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    16                          n/a    n/a               pi                     ppio.compxrcCJO...///wESDgic5BD+ /////////8                     B
                   1994-09-09 13:56:00  1970-01-01 00:00:00       1970-01-01 00:00:00             0      0
    15                          n/a    n/a               ad                     n                                xs.comsess                     1
                   1994-08-29 04:30:38  1970-01-01 00:00:00       1970-01-01 00:00:00             0      1
    15                          n/a    n/a               acniv                  alist.comavlukey5a78889          3caf7a1.51970462.d             c
```

Probaremos de extraer los ficheros en uso por parte del proceso explorer.exe con PID 1900:

```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles -n -p 1900 -D ./explorer1900
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0xfffffa8002dcd070   1900   \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
SharedCacheMap 0xfffffa8002dcd070   1900   \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
DataSectionObject 0xfffffa8002df95c0   1900   \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windo
4144ccf1df_6.0.7600.16385_es-es_103af8cc43d0a688\comctl32.dll.mui
DataSectionObject 0xfffffa80019e8d40   1900   \Device\HarddiskVolume2\Windows\System32\es-ES\ActionCenter
DataSectionObject 0xfffffa8002e88690   1900   \Device\HarddiskVolume2\Windows\System32\es-ES\KernelBase.d
DataSectionObject 0xfffffa8001d77520   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
r.db
DataSectionObject 0xfffffa8001d77ac0   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
6.db
DataSectionObject 0xfffffa8001d77700   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
024.db
DataSectionObject 0xfffffa8001ad2c80   1900   \Device\CdRom0\
SharedCacheMap 0xfffffa8001ad2c80   1900   \Device\CdRom0\
DataSectionObject 0xfffffa8001d778e0   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
56.db
DataSectionObject 0xfffffa8002970350   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
2.db
DataSectionObject 0xfffffa8001d76960   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
dx.db
DataSectionObject 0xfffffa80028c5570   1900   \Device\HarddiskVolume2\Windows\System32\locale.nls
DataSectionObject 0xfffffa8002924510   1900   \Device\HarddiskVolume2\Windows\Globalization\Sorting\SortD
DataSectionObject 0xfffffa8002be1070   1900   \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Cache
DataSectionObject 0xfffffa8002be8860   1900   \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Cache
9AF493}.2.ver0x0000000000000011.db
DataSectionObject 0xfffffa8002dfb070   1900   \Device\HarddiskVolume2\Users\unaalmes\AppData\Local\Micros
-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000003.db
DataSectionObject 0xfffffa8002c8ea50   1900   \Device\HarddiskVolume2\Windows\System32\msxml6r.dll
DataSectionObject 0xfffffa8002beedc0   1900   \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Cache
C3FDA2}.2.ver0x0000000000000002.db
DataSectionObject 0xfffffa8002e1ff20   1900   \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Cache
66C508}.2.ver0x0000000000000001.db
DataSectionObject 0xfffffa8002b252c0   1900   \Device\HarddiskVolume2\Windows\System32\oleaccrc.dll
ImageSectionObject 0xfffffa8002a6d290   1900   \Device\HarddiskVolume2\Windows\System32\imageres.dll
```

Extrae 189 ficheros, pero ninguno de ellos con extensión previsible de ser analizada. Casi todo dll's i algún .db de thumbnails.

Lo probamos también con el proceso explorer.exe con PID 2692 pero obtenemos el mismo resultado.

Listamos los archivos en memoria buscando alguno que pueda servirnos para empezar a tirar del hilo.

Como la lista es larga filtramos en las carpetas del usuario.

Carpeta descargas:

```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 filescan | grep Downloads
Volatility Foundation Volatility Framework 2.6
0x000000007eaf72d0      1      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Links\Downloads.lnk
0x000000007ec5b180      1      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\desktop.ini
0x000000007fb09bf0      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads
0x000000007fb22d50      2      0 RWD--- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt.zip
0x000000007fb361c0      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt
0x000000007fb52530     14      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
0x000000007fb78950     15      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\MagnetRAMCapture.exe
0x000000007fb78d10     14      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\Apache_OpenOffice_4.1.4_Win_x86_install_es.exe
0x000000007fb7c540      1      1 RW-rw- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\UNAALMES-PC-20180915-095618.raw
0x000000007fcdd3c0      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads
0x000000007fd30cf0      2      0 -W-r-- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\README.txt
0x000000007fd347c0      1      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
0x000000007fd36d50     16      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\DumpIt.exe
0x000000007fd37b20     16      0 -W-r-- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\DumpIt.exe
0x000000007fd44350      1      1 R--rw- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt
0x000000007fed4dd0      1      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
0x000000007fed5720      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt
```

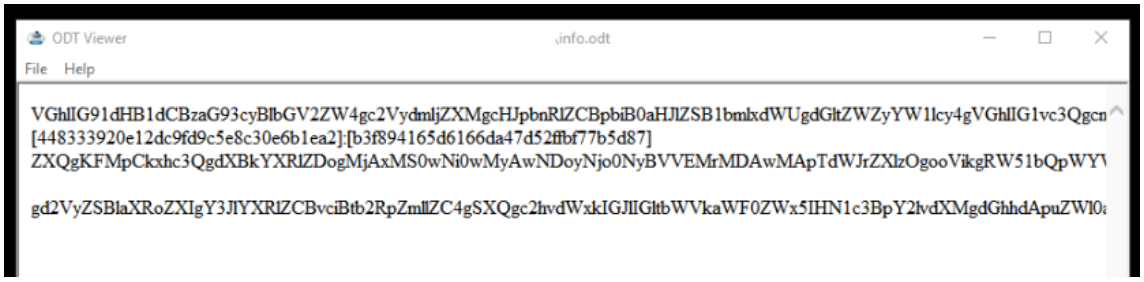
Observamos que se ha descargado el WinRar, el OpenOffice y el DumpIt para realizar la captura de la memoria. Parece ser que el fichero va a ser de formato OpenOffice….

En la carpeta Documentos no hay ningún documento, así que probamos en el escritorio:

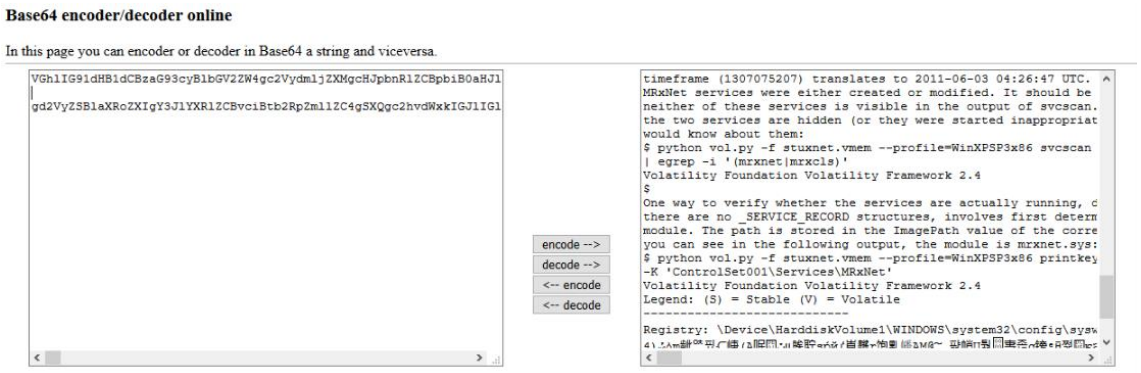
```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 filescan | grep Desktop'\\'
Volatility Foundation Volatility Framework 2.6
0x000000007e807520      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit
0x000000007e82b180      2      0 R--rw- \Device\HarddiskVolume2\Users\unaalmes\Desktop\IDA Pro (64-bit).lnk
0x000000007e82b680      2      0 R--rw- \Device\HarddiskVolume2\Users\Public\Desktop\Firefox.lnk
0x000000007e82ca10     16      0 R--rw- \Device\HarddiskVolume2\Users\unaalmes\Desktop\IDA Pro (32-bit).lnk
0x000000007e82de20     16      0 R--rw- \Device\HarddiskVolume2\Users\Public\Desktop\OpenOffice 4.1.4.lnk
0x000000007e9d8af0     12      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\DumpIt_1734677328.exe
0x000000007eb48e00      2      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\RamCaptureDriver64.sys
0x000000007ebfbbe0     16      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\desktop.ini
0x000000007ec6bac0      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit
0x000000007eddc540     16      0 R--rwd \Device\HarddiskVolume2\Users\Public\Desktop\desktop.ini
0x000000007fae4680     16      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\RamCaptureDriver64.sys
0x000000007faee900     15      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\msvcp110.dll
0x000000007fafb440      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer
0x000000007fb02430      2      1 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer
0x000000007fb0e2c0      6      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\msvcr110.dll
0x000000007fca5580      2      0 RW-rw- \Device\HarddiskVolume2\Users\unaalmes\Desktop\.~lock.info.odt#
0x000000007fcabd50      1      1 RW-r-- \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
0x000000007fcdf8d0     11      0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\RamCapture64.exe
0x000000007fce3860     11      0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Desktop\RamCapturer\64bit\RamCapture64.exe
```

Parece que empezamos a ver la luz. Hay un fichero llamado *'info.odt'* de OpenOffice. Así que toca obtenerlo a partir de su offset físico y abrirlo:

```
>volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007fcabd50 -n -u -S resultado.txt -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7fcabd50   None   \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
>file info.odt
info.odt: OpenDocument Text
>
```




Parece ser que esta codificado en base 64. Probamos a copiar su contenido y ver que obtenemos:



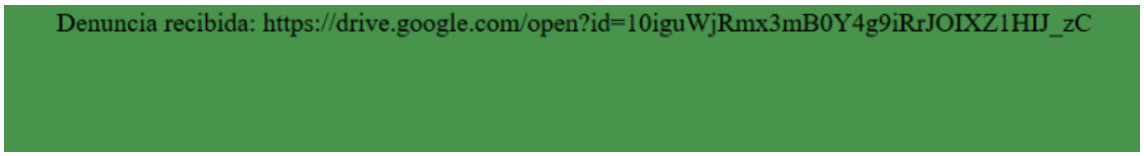

Pues parece la salida de una ejecución de volatility. Aunque vemos que a partir de ciertos caracteres la salida se empieza a mostrar ilegible, lo que nos da que pensar.

Volviendo al fichero info.odt observamos que tiene un par de caracteres alfanuméricos entre corchetes (lo que rompe la codificación en base 64):

[448333920e12dc9fd9c5e8c30e6b1ea2]:[b3f894165d6166da47d52ffbf77b5d87]

Parecen dos cadenas MD5. Vamos a ver si encontramos alguna web que las decodifique. Probamos en la plataforma https://md5online.org/ y obtenemos resultado: **[Gilfoyle]:[Satan]**

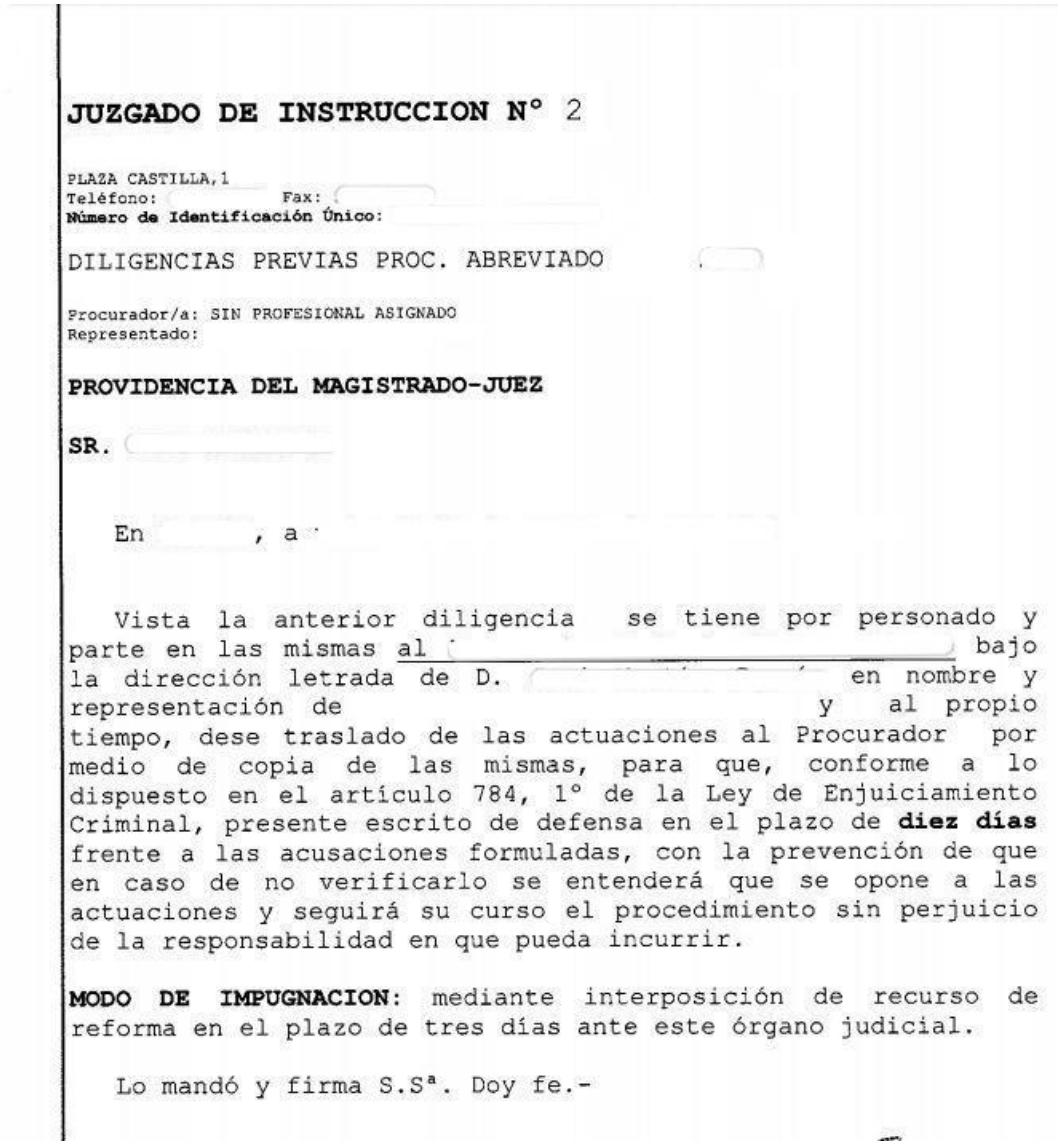
Probamos de loguearnos en la url http://34.247.69.86/siliconvalley/episodio1/login.php con los datos anteriores y accedemos:


Así que a por el siguiente paso.

## PARTE 2 – METADATA

Accedemos a la url obtenida https://drive.google.com/open?id=10iguWjRmx3mB0Y4g9iRrJOIXZ1HIJ_zC y obtenemos un archivo jpeg *'denuncia.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.

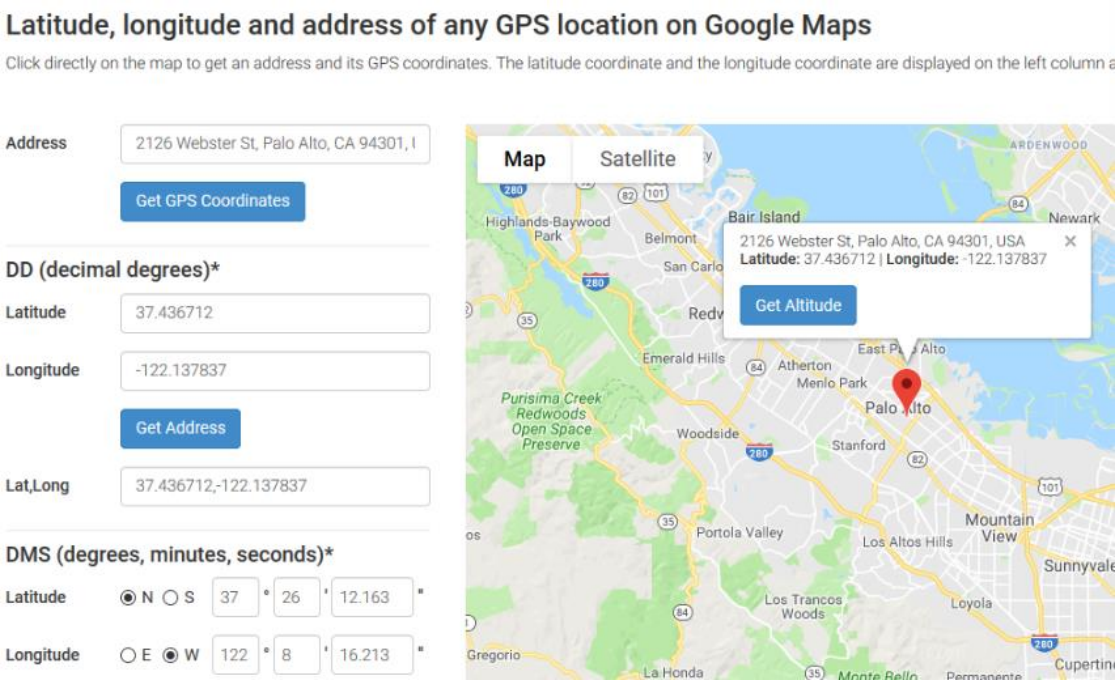
Lo mandó y firma S.Sª. Doy fe.-

Probamos modificar la saturación, brillo y abrirlo con diferentes paletas con el programa *Gimp* por si hay algo escondido, pero no obtenemos resultado.

Probamos con sus metadatos con el comando *'exiftool'*:

```
>exiftool denuncia.jpeg
ExifTool Version Number         : 11.10
File Name                       : denuncia.jpeg
Directory                       : .
File Size                       : 177 kB
File Modification Date/Time     : 2018:09:17 15:03:39+02:00
File Access Date/Time           : 2018:09:17 15:03:37+02:00
File Inode Change Date/Time     : 2018:09:17 15:04:02+02:00
File Permissions                : rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
XMP Toolkit                     : Image::ExifTool 11.10
Location                        : 37.436712, -122.137837
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
```

Vemos que tiene un metadato con la ubicación y sus coordenadas 37.436712, -122.137837.
Vamos a ver su dirección física:



Pues ya sabemos que la ubicación está en Palo Alto, y el número es el 2126:


Como la flag era obtener el numero de la casa en formato md5, el resultado será codificar 2126 en ese formato:

**UAM{3b92d18aa7a6176dd37d372bc2f1eb71}**

# REFERENCIAS

**Plugin Firefox Volatility:**

https://github.com/superponible/volatility-plugins

**Codificadores:**

http://multiencoder.com/

https://md5online.org/

http://www.utilities-online.info/base64/

Coordenadas:

https://www.gps-coordinates.net/