UAM SILICON VALLEY – EPISODIO 1

Jose Ignacio de Miguel González (User: nachinho3)

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-_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}

Descargamos el fichero, y lo descomprimimos, y es un fichero raw de 2 GB:

Si miramos sus cabeceras, no nos dice mucho, aunque parece que es una imagen de Virtual BOX:

```
nacho@kali:/media/sf_Compartir/CCN$ hexdump -C GILFOYLE-HELLDD.raw | more
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001000  00 c0 d0 ff ff ff ff ff  00 30 d0 ff ff ff ff ff  |.........0......|
00001010  f0 00 ff 7f 00 00 00 00  46 41 43 50 f4 00 00 00  |........FACP....|
00001020  04 00 56 42 4f 58 20 20  56 42 4f 58 46 41 43 50  |..VBOX  VBOXFACP|
00001030  01 00 00 00 41 53 4c 20  61 00 00 00 00 02 ff 7f  |....ASL a.......|
00001040  70 04 ff 7f 00 00 09 00  2e 44 00 00 a1 a0 00 00  |p........D......|
00001050  00 40 00 00 00 00 00 00  04 40 00 00 00 00 00 00  |.@.......@......|
00001060  00 00 00 00 08 40 00 00  20 40 00 00 00 00 00 00  |.....@.. @......|
00001070  04 02 00 04 02 00 00 00  65 00 e9 03 00 00 00 00  |........e.......|
00001080  00 00 00 00 00 03 00 00  41 05 00 00 01 08 00 01  |........A.......|
00001090  50 40 00 00 00 00 00 00  10 00 00 00 00 02 ff 7f  |P@..............|
000010a0  00 00 00 00 70 04 ff 7f  00 00 00 00 01 20 00 02  |....p........ ..|
000010b0  00 40 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.@..............|
000010c0  00 00 00 00 01 10 00 02  04 40 00 00 00 00 00 00  |.........@......|
000010d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Vamos a intentar buscar cosas dentro del fichero con volatility. Intentamos identificar el tipo de fichero con la opción crashinfo, pero no nos reconoce un sistema conocido:

```
nacho@kali:/media/sf_Compartir/CCN$ volatility -f GILFOYLE-HELLDD.raw crashinfo --profile Wi
n7SP1x64
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Memory Image could not be identified as ['WindowsCrashDumpSp
ace32', 'WindowsCrashDumpSpace64', 'WindowsCrashDumpSpace64BitMap']
```

Sin embargo, si hacemos un listado de ficheros si que nos devuelve una gran cantidad de ellos. Los sacamos a fichero para poder verlos con calma:

```
nacho@kali:/media/sf_Compartir/CCN$ volatility -f GILFOYLE-HELLDD.raw filescan --profile Win
7SP1x64 > ficherosUAM.txt
Volatility Foundation Volatility Framework 2.6
```

Encontramos un ejecutable, dentro del directorio del usuario “unaalmes” que tiene posibilidades:

```
0x000000007e9d8af0      12      0 R--r-d \Device\HarddiskVolume2\Users
\unaalmes\Desktop\DumpIt_1734677328.exe
```

Vamos a extraerlo:

```
nacho@kali:/media/sf_Compartir/CCN$ volatility -f GILFOYLE-HELLDD.raw  --profile=Win7SP1x64 d
umpfiles --dump-dir=filesDump -Q 0x000000007e9d8af0
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x7e9d8af0   None   \Device\HarddiskVolume2\Users\unaalmes\Desktop\DumpIt_
1734677328.exe
DataSectionObject 0x7e9d8af0   None   \Device\HarddiskVolume2\Users\unaalmes\Desktop\DumpIt_1
734677328.exe
```

Nos ha recuperado dos ficheros:

```
nacho@kali:/media/sf_Compartir/CCN/filesDump$ ls -la
total 1088
drwxrwx--- 1 root vboxsf       0 sep 15 20:41 .
drwxrwx--- 1 root vboxsf    4096 sep 15 20:38 ..
-rwxrwx--- 1 root vboxsf   57856 sep 15 20:41 file.None.0xfffffa8001ce72d0.img
-rwxrwx--- 1 root vboxsf 1048576 sep 15 20:41 file.None.0xfffffa8001d12c00.dat
```

Si editamos cada uno a ver lo que es, el segundo es un ejecutable:

```
00000000  4d 5a 50 00 02 00 00 00  04 00 0f 00 ff ff 00 00  |MZP.............|
00000010  b8 00 00 00 00 00 00 00  40 00 1a 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00  |................|
00000040  ba 10 00 0e 1f b4 09 cd  21 b8 01 4c cd 21 90 90  |........!..L.!..|
00000050  54 68 69 73 20 70 72 6f  67 72 61 6d 20 6d 75 73  |This program mus|
00000060  74 20 62 65 20 72 75 6e  20 75 6e 64 65 72 20 57  |t be run under W|
00000070  69 6e 33 32 0d 0a 24 37  00 00 00 00 00 00 00 00  |in32..$7........|
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000100  50 45 00 00 4c 01 08 00  19 5e 42 2a 00 00 00 00  |PE..L....^B*....|
00000110  00 00 00 00 e0 00 8f 81  0b 01 02 19 00 9e 00 00  |................|
00000120  00 46 00 00 00 00 00 00  f8 a5 00 00 00 10 00 00  |.F..............|
00000130  00 b0 00 00 00 00 40 00  00 10 00 00 00 02 00 00  |......@.........|
```

Nos lo llevamos a Windows, pero al ejecutarlo no hace nada. Consultando por Internet es una utilidad para poder hacer volcados de memoria, por lo que no es lo que realmente estamos buscando. Continuamos la búsqueda.

Un tema sospechoso es que, dentro de la máquina, vemos que ha descargado varios archivos ejecutables, todos relacionados con la propia captura de memoria. Sin embargo, vemos que también ha descargado el OpenOffice, ¿para qué lo querría?

```
/CCN$ more ficherosUAM.txt | grep "Downloads" | grep "exe" | more
 0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
 0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\MagnetRAMCapture.exe
 0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\Apache_OpenOffice_4.1.4_Win_x86_install_es.exe
 0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
 0 R--r-d \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\DumpIt.exe
 0 -W-r-- \Device\HarddiskVolume2\Users\unaalmes\Downloads\DumpIt\DumpIt.exe
 0 R--rwd \Device\HarddiskVolume2\Users\unaalmes\Downloads\winrar-x64-550es.exe
```

Filtrando a su vez por el usuario “unaalmes”, encontramos un fichero de tipo ODT (OpenOffice texto), llamado info.odt. Ese fichero puede contener la información que buscamos, así que lo recuperamos:

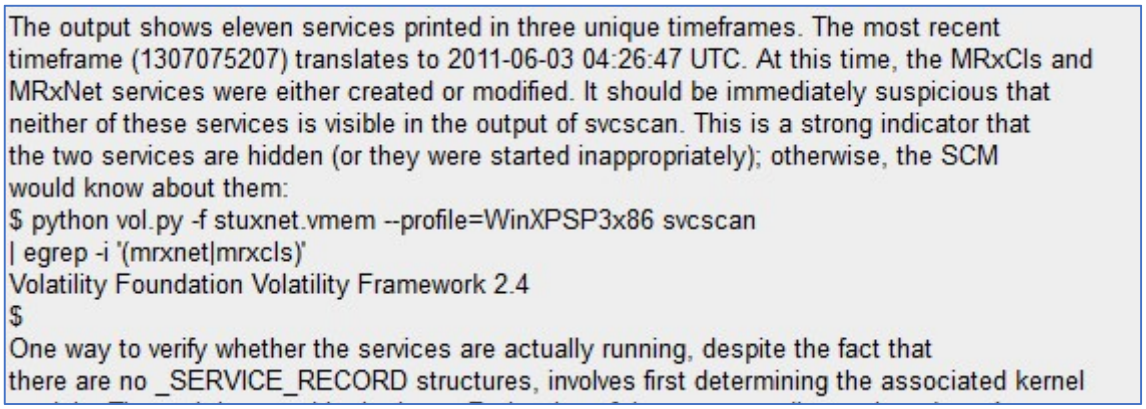
```
nacho@kali:/media/sf_Compartir/CCN$ volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles
--dump-dir=filesDump -Q 0x000000007fcabd50
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7fcabd50   None   \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
```

Nos genera un fichero .dat que renombramos a info.odt. Si lo editamos, nos confirma que es un fichero ODT (internamente es un fichero ZIP):

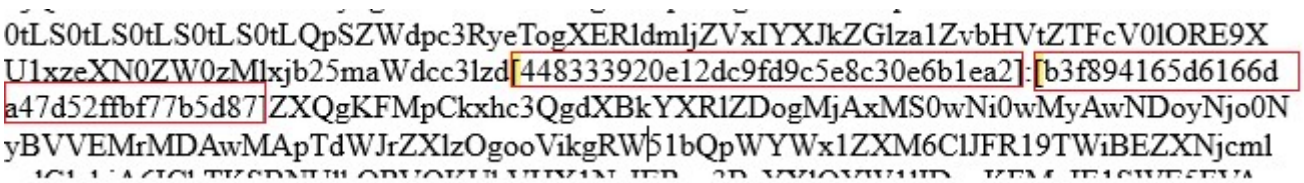
```
nacho@kali:/media/sf_Compartir/CCN$ hexdump -C  info.odt | more
00000000  50 4b 03 04 14 00 00 08  00 00 d0 4e 2f 4d 5e c6  |PK.........N/M^.|
00000010  32 0c 27 00 00 00 27 00  00 00 08 00 00 00 6d 69  |2.'...'.......mi|
00000020  6d 65 74 79 70 65 61 70  70 6c 69 63 61 74 69 6f  |metypeapplicatio|
00000030  6e 2f 76 6e 64 2e 6f 61  73 69 73 2e 6f 70 65 6e  |n/vnd.oasis.open|
00000040  64 6f 63 75 6d 65 6e 74  2e 74 65 78 74 50 4b 03  |document.textPK.|
00000050  04 14 00 08 08 08 00 d0  4e 2f 4d 00 00 00 00 00  |........N/M.....|
00000060  00 00 00 00 00 00 00 27  00 00 00 43 6f 6e 66 69  |.......'...Confi|
00000070  67 75 72 61 74 69 6f 6e  73 32 2f 61 63 63 65 6c  |gurations2/accel|
00000080  65 72 61 74 6f 72 2f 63  75 72 72 65 6e 74 2e 78  |erator/current.x|
00000090  6d 6c 03 00 50 4b 07 08  00 00 00 00 02 00 00 00  |ml..PK..........|
000000a0  00 00 00 00 50 4b 03 04  14 00 00 08 00 00 d0 4e  |....PK.........N|
000000b0  2f 4d 00 00 00 00 00 00  00 00 00 00 00 00 1f 00  |/M..............|
000000c0  00 00 43 6f 6e 66 69 67  75 72 61 74 69 6f 6e 73  |..Configurations|
000000d0  32 2f 69 6d 61 67 65 73  2f 42 69 74 6d 61 70 73  |2/images/Bitmaps|
000000e0  2f 50 4b 03 04 14 00 00  08 00 00 d0 4e 2f 4d 00  |/PK.........N/M.|
000000f0  00 00 00 00 00 00 00 00  00 00 00 18 00 00 00 43  |...............C|
00000100  6f 6e 66 69 67 75 72 61  74 69 6f 6e 73 32 2f 66  |onfigurations2/f|
00000110  6c 6f 61 74 65 72 2f 50  4b 03 04 14 00 00 08 00  |loater/PK.......|
00000120  00 d0 4e 2f 4d 00 00 00  00 00 00 00 00 00 00 00  |..N/M...........|
00000130  00 1c 00 00 00 43 6f 6e  66 69 67 75 72 61 74 69  |.....Configurati|
00000140  6f 6e 73 32 2f 70 72 6f  67 72 65 73 73 62 61 72  |ons2/progressbar|
00000150  2f 50 4b 03 04 14 00 00  08 00 00 d0 4e 2f 4d 00  |/PK.........N/M.|
```

Nos lo llevamos a Word y lo abrimos, pese a que da un error de formato cuando lo abrimos nos saca varias páginas de un texto que parece base64:

Vemos que entre todo ese texto, hay algunos caracteres “/”, cogemos toda la primera parte y hacemos el “decode” de base64, lo cual vemos que es legible:



Sin embargo, de dicho texto no puedo sacar nada que parezcan unas credenciales. Sigo buscando y veo que hay unos caracteres “[“ y “]”, separados con un “:”. Dentro de esos caracteres, veo dos cadenas de 32 bytes, que podrían ser un MD5:

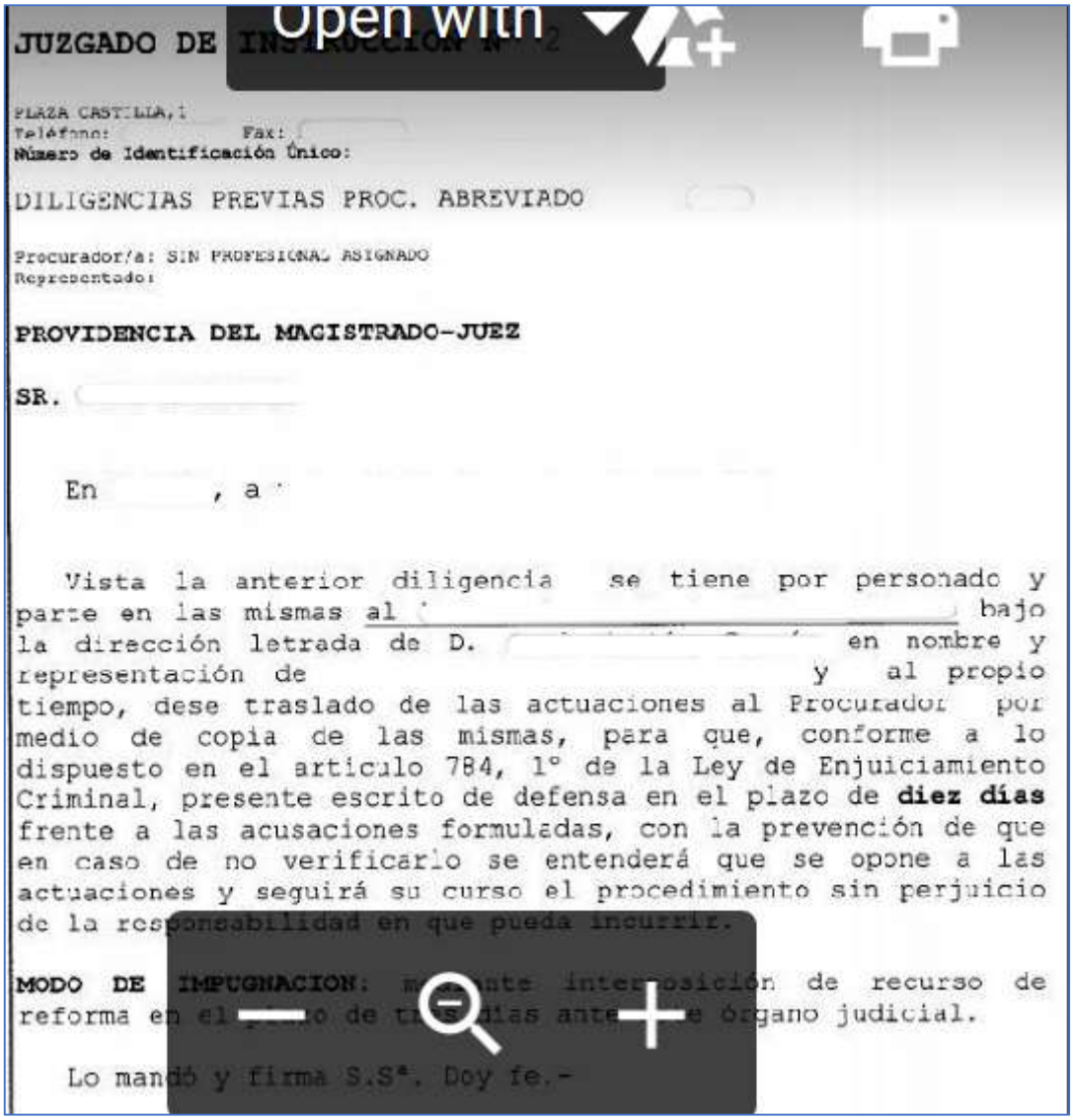


Buscamos ambas cadenas en un crackeador de MD5 y obtenemos resultados:

Por tanto, podrían ser el usuario y password que buscamos. Nos vamos a la Web del reto y lo probamos:

Perfecto!, entramos en la Web y nos devuelve una URL de descarga:

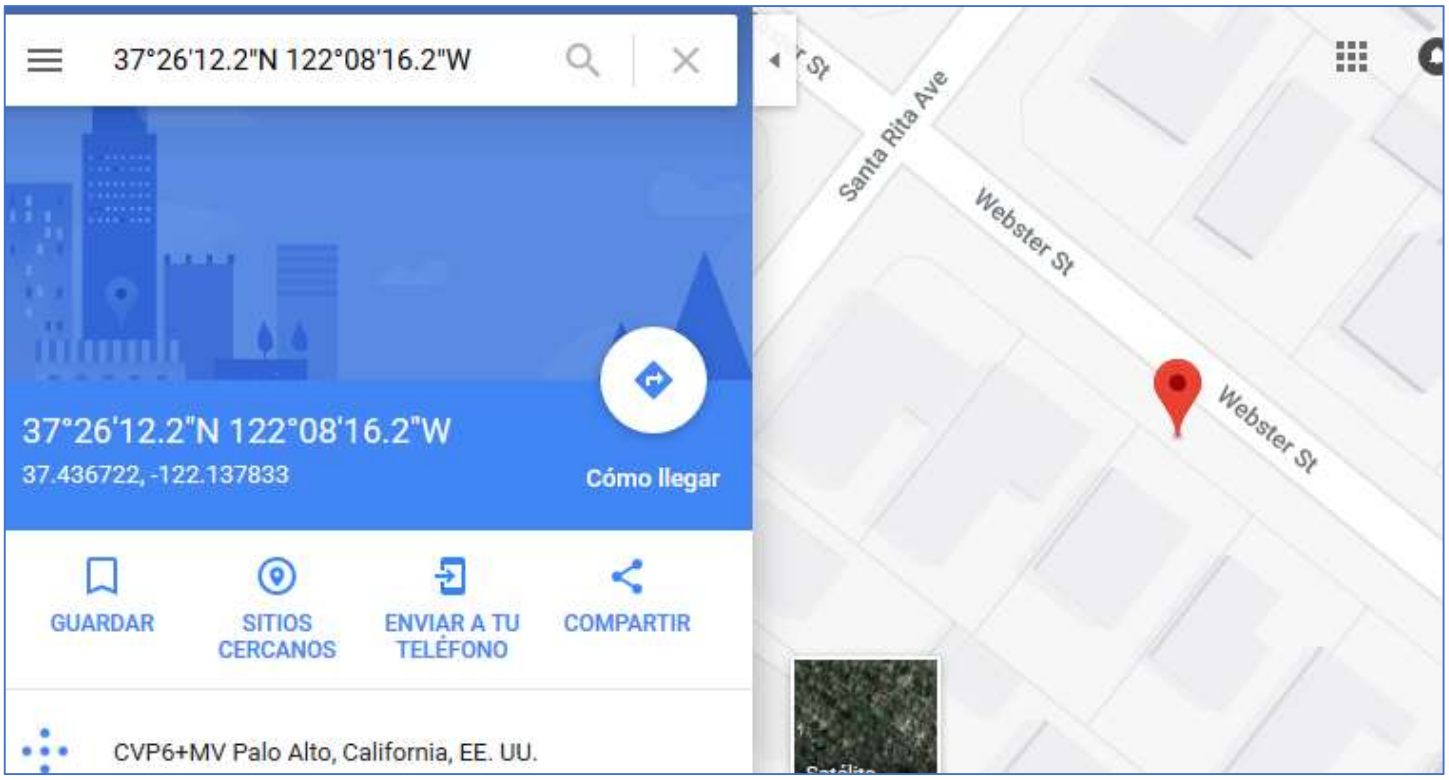
Al descargarla, es una imagen, con un texto que parece una denuncia. La abrimos y buscamos una dirección:



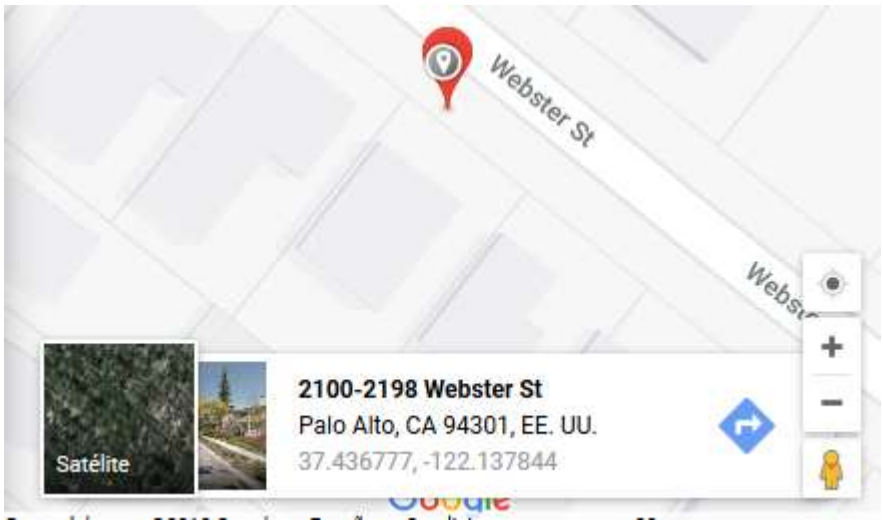
En la imagen no hay ninguna dirección, ni ningún dato del que podamos tirar. Vamos a mirar en sus metadatos, por si estuviera ahí:

```
nacho@kali:/media/sf_Compartir/CCN$ exiftool denuncia.jpeg
ExifTool Version Number         : 10.96
File Name                       : denuncia.jpeg
Directory                       : .
File Size                       : 177 kB
File Modification Date/Time     : 2018:09:16 15:32:17+02:00
File Access Date/Time           : 2018:09:16 15:34:59+02:00
File Inode Change Date/Time     : 2018:09:16 15:32:17+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
XMP Toolkit                     : Image::ExifTool 11.10
Location                        : 37.436712, -122.137837
Profile CMM Type                : Unknown (lcms)
```

En los metadatos, vemos unas coordenadas de una localización, nos las llevamos a Google Maps:



En el plano no viene ningún número de casa, ni de calle. Solo el nombre de la calle. Pincho en la chincheta del marcador, y nos indica unos números al lado del nombre de la calle (2100-2198):



Pincho en el icono de StreetView, a ver si puedo ver algo dentro. Nos muestra una casa a la izquierda, y si hacemos zoom, vemos que en la puerta tiene un número:

Ese número 2126 es la FLAG, por tanto, si componemos la forma final con el MD5 sería:
UAM{3b92d18aa7a6176dd37d372bc2f1eb71}