

# Una al Mes (Mission 005)

@percu

20/03/18

## Contenido

INTRODUCCIÓN .....	1
MISIÓN .....	2
RESOLUCIÓN.....	3
PARTE 1 - WEB .....	3
PARTE 2 - ESTEGANOGRAFIA .....	5
PARTE 3 – ANÁLISIS FORENSE.....	8
REFERENCIAS .....	18

## INTRODUCCIÓN

Puesto que es de mis primeros CTF, este *write-up* tiene un enfoque más práctico que técnico.

El motivo es tener una futura referencia de las herramientas utilizadas, así como las deducciones que he ido aplicando cuando me he quedado estancado.

Por lo tanto, más que la explicación de los pasos realizados para la resolución del CTF, este *write-up* es un *time-line* de como he ido solucionado los diferentes retos propuestos, aunque también identifico los palos de ciego que he ido dando mientras me quedaba estancado en cada uno de los retos y como le daba la vuelta para encontrar su solución.

Empecemos...

## MISIÓN

En la URL <http://34.253.233.243/mission5.php> encontramos la información:

### Mission#005

#### Información personal:

**Nombre:** Thomas A. Anderson

**Fecha de nacimiento:** 11 de Marzo del 1962

**Trabajo:** Programador

**Empresa:** Metacortex



#### Misión:

**Nivel:** Medio

#### Introducción:

¡Neo, tenemos un problema! Han secuestrado a Morfeo y no sabemos dónde lo pueden tener. Necesitamos que investigues y descubras su localización para rescatarlo. La única pista que tenemos es una URL que conseguimos. ¿Serás capaz de encontrarle?

#### Información adicional:

**URL conseguida:** <http://34.253.233.243/search/localizacion.php>

**Tip:** La flag es el nombre del sitio donde se encuentra con el formato UAM{Localización}.

**Tip2:** El nombre del sitio en la flag es con "\_" en lugar de espacios.

**Tip3:** El archivo ".zip" se descomprime con "123mango".

**Tip4:** Hay una flag trampa la cuál no tiene localización.

## RESOLUCIÓN

### PARTE 1 - WEB

Al acceder a la url <http://34.253.233.243/search/localizacion.php> solamente encontramos un gif de Neo con la frase “No todo es lo que parece...”:



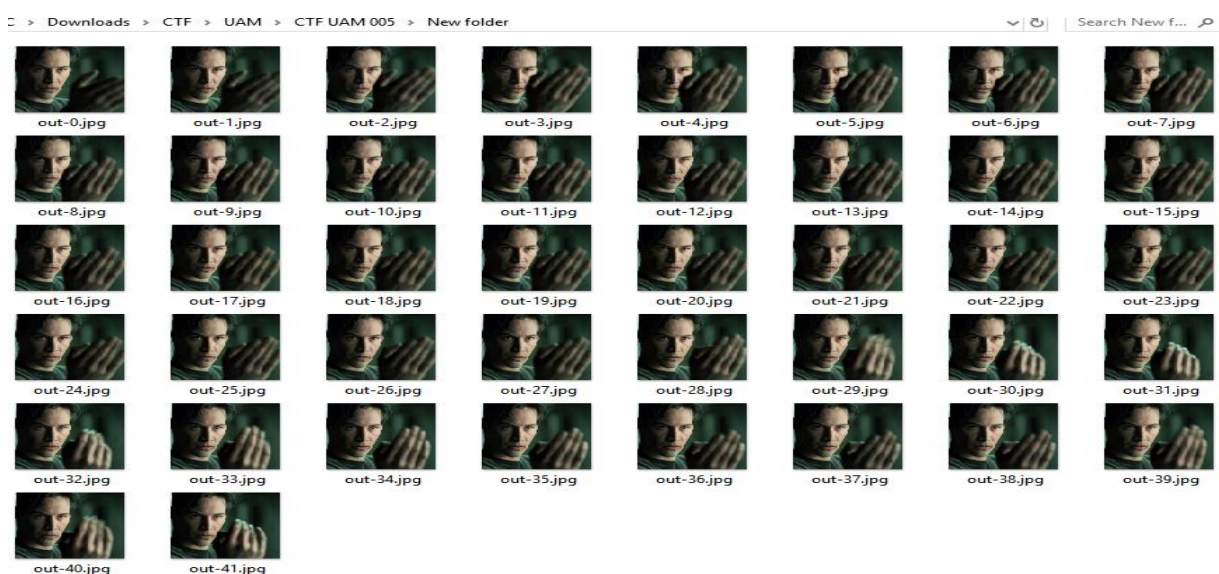
En principio parece un reto de esteganografía, por lo que procedemos a descargar el gif i revisarlo.

Con la utilidad ‘*steghide*’ miramos si hay información escondida, pero no encontramos nada:

```
> steghide info neo.gif
steghide: the file format of the file "neo.gif" is not supported.
```

Con el comando ‘*convert*’ de *ImageMagick* obtenemos todas las imágenes del gif, pero no encontramos nada... salvo a Neo saludando en todas las posiciones posibles:

```
#: convert -coalesce neo.gif out.jpg
```



Miramos las propiedades de los archivos '\*.jpg' obtenidos, pero sin encontrar nada de interés.

Se parecía que al cargar la url hace previamente una llamada, por lo que vamos a intentar descargar la url principal con el comando 'wget':

```
#: wget http://34.253.233.243/search/localizacion.php
```

Vemos que el código .php obtenido tiene como título "Archivo de localización encriptado" y después de muchos tags <br> hay escondidas dos url's y la indicación de que tenemos que sacar información del primer archivo para pasársela al segundo

```
<br>
</html>
Para continuar deberéis sacar X información del primer archivo (la cuál está encriptada) y pasársela al segundo:
<br>Archivo 1: https://goo.gl/K1dcbG <br>Archivo 2: https://drive.google.com/open?id=1CAz5xxsf9YxGLSWDgOVURsvFmT6A1Sw
n <br>
>
```

En la primera url <https://goo.gl/K1dcbG> obtenemos el Archivo 1 morfeo.jpg



Y en la segunda url <https://drive.google.com/open?id=1CAz5xxsf9YxGLSWDgOVURsvFmT6A1Swn> el fichero web.py:

```
#!/usr/bin/python3
string = input("Introduce la información que hayas sacado de la imagen: ")

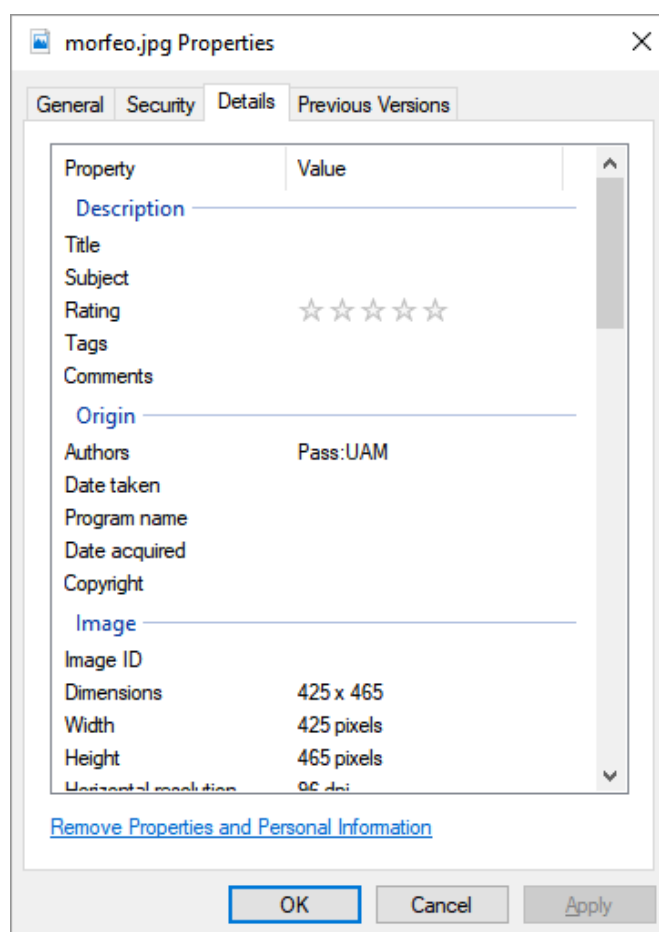
a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r = string
a = a.lower()
b = b.lower()
c = c.lower()
d = d.lower()
e = e.lower()
f = ':'/'/'
g = g.lower()
h = h.lower()
i = i.lower()
j = '.'
k = k.lower()
l = l.lower()
m = '/'
n = n.upper()
o = o.lower()
p = p.upper()
q = q.upper()
r = r.lower()
s = '2'
print (a + b + c + d + e + f + g + h + i + j + k + l + m + n + o + p + q + r + s)
```

## PARTE 2 - ESTEGANOGRAFIA

Analizando el fichero 'morfeo.jpg' con la utilidad 'steghide' vemos que tiene información oculta y nos pide contraseña:

```
> steghide info morfeo.jpg
"morfeo.jpg":
  format: jpeg
  capacity: 1.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
> _
```

Si miramos sus propiedades vemos que la tiene en los metadatos del fichero:



Ponemos dicho password y vemos que tiene un fichero 'morfeo.txt' oculto en la imagen:

```
> steghide info morfeo.jpg
"morfeo.jpg":
  format: jpeg
  capacity: 1.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "morf.txt":
    size: 78.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Extraemos dicho fichero y miramos su contenido:

```
> rsteghide extract -sf morfeo.jpg
Enter passphrase:
wrote extracted data to "morf.txt".
> more morf.txt
AABBBBAABBBBAABBBBBAABA AABBAABBBBAABBBBA AABBAABABB AABABABABABAAAABAAAABA
```

Esta cadena de caracteres es la que tendremos que pasarle al script Python ‘web.py’ descargado anteriormente tal y como nos indicaban...

Al ejecutar el script en Python nos pide la información extraída de la imagen anterior y si ponemos el contenido del fichero ‘morf.txt’ nos responde diciendo que tenemos que poner 18 caracteres:

```
>python web.py
Introduce la informacion que hayas sacado de la imagen: AABBBBAABBBBAABBBBBAABA AABBAABBBBAABBBBA AABBAABABB AABABABABABAAAABAAAABA
Traceback (most recent call last):
  File "web.py", line 5, in <module>
    a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r = string
ValueError: too many values to unpack (expected 18)
```

Observando el script se ve como el sexto carácter lo sustituye por “: //”, el décimo por “.”, el treceavo por “/” y le añade un “2” al final. Parece que sea el formato de una url, así que nos fijaremos en los primeros 5 caracteres:

```
a = a.lower()
b = b.lower()
c = c.lower()
d = d.lower()
e = e.lower()
f = ': //'
```

Podemos deducir que el primer carácter tiene que ser una ‘H’, el segundo y tercero una ‘T’, el cuarto una ‘P’ i el quinto una ‘S’.

A partir del contenido del fichero ‘morf.txt’ vemos que las cadenas formadas por las letras ‘A’ y ‘B’ forman 4 grupos, los mismos que hay en el script en Python.

Con el primer grupo (AABBBBAABBBBAABBBBBAABA) debemos formar 5 caracteres, así que dividimos la cadena en 5 trozos iguales:

AABBB, BAABB, BAABB, ABBBB, BAABA

Ya vemos que el segundo y tercer grupo son iguales, por lo que el patrón deducido de https parece ser correcto. Solo falta averiguar valores...

Si convertimos a binario suponiendo que la ‘B’ tiene valor ‘1’ y la ‘A’ valor ‘0’ obtenemos:

7, 19, 19, 15, 18

Si tomamos el abecedario con la letra A=0, nos queda H, T, T, P, S dando la cadena correcta.

Solamente nos queda transformar cada grupo de 5 letras del fichero ‘*morf.txt*’ a binario y buscar su valor en el abecedario:

GRUPO 1	GRUPO 2	GRUPO 3	GRUPO 4
AABBB - 7 - h BAABB - 19 - t BAABB - 19 - t ABBBB - 15 - p BAABA - 18 - s	AABBA - 6 - g ABBBA - 14 - o ABBBA - 14 - o	AABBA - 6 - G ABABB - 11 - L	AABAB - 5 - f ABABA - 10 - k BAAAA - 16 - q BAAAB - 17 - r AAABA - 2 - c

Le pasamos la cadena obtenida (https goo gl fkqrc) al script Python:

```
>python web.py
Introduce la información que hayas sacado de la imagen: https goo gl fkqrc
https://goo.gl/FkQRc2
```

Y obtenemos la url: <https://goo.gl/FkQRc2>



### PARTE 3 – ANÁLISIS FORENSE

En la dirección anterior <https://goo.gl/FkQRc2> nos podemos descargar un fichero de nombre ‘*morfeo.zip*’ comprimido, del cual nos dan la contraseña en un *tip* (123Mango)

Dentro de ese fichero comprimido hay otro de nombre *morfeo.dmp* que parece ser un volcado de memoria. Lo analizamos con la herramienta ‘*volatility*’

```
>volatility -f morfeo.dmp imageinfo
Suggested Profile(s) : Win8SP0x64, Win81U1x64, Win10x64_14393, Win2012R2x64_18340, Win10x64,
Win2016x64_14393, Win2012R2x64, Win2012x64, Win8SP1x64_18340, Win10x64_10586, Win8SP1x64, Win10x64_15063
(Instantiated with Win10x64_15063)
AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
AS Layer2 : WindowsCrashDumpSpace64 (Unnamed AS)
AS Layer3 : FileAddressSpace (/mnt/c/morfeo.dmp)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800028040a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff80002805d00L
KUSER_SHARED_DATA : 0xffffffff7800000000L
Image date and time : 2018-03-12 20:35:20 UTC+0000
Image local date and time : 2018-03-12 21:35:20 +0100
```

Vemos que es de un sistema Windows de 64bits. Procedemos a mirar con qué profile examinarla con el plugin ‘*kdbgscan*’, que lo instancia con todos los *profiles* posibles (recorto salida de pantalla porque es extensa):

```
>volatility -f morfeo.dmp kdbgscan
*****
Instantiating KDBG using: Kernel AS Win10x64_14393 (6.4.14393 64bit)
Offset (V) : 0xf800028040a0
Offset (P) : 0x28040a0
KdCopyDataBlock (V) : 0xf8000271bc04
Block encoded : No
Wait never : 0xb79180109e1676c0
Wait always : 0x84f0f5ea6bc9180
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win10x64_14393
Version64 : 0xf80002804068 (Major: 15, Minor: 7601)
Service Pack (CmNtCSDVersion) : 1
Build string (NtBuildLab) : 7601.17514.amd64fre.win7sp1_rtm.
PsActiveProcessHead : 0xffffffff8000283ab90 (37 processes)
PsLoadedModuleList : 0xffffffff80002858e90 (139 modules)
KernelBase : 0xffffffff80002613000 (Matches MZ: True)
Major (OptionalHeader) : 6
Minor (OptionalHeader) : 1
KPCR : 0xffffffff80002805d00 (CPU 0)
*****
Instantiating KDBG using: Kernel AS Win10x64 (6.4.9841 64bit)
Offset (V) : 0xf800028040a0
Offset (P) : 0x28040a0
KdCopyDataBlock (V) : 0xf8000271bc04
Block encoded : No
Wait never : 0xb79180109e1676c0
Wait always : 0x84f0f5ea6bc9180
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win10x64
Version64 : 0xf80002804068 (Major: 15, Minor: 7601)
Service Pack (CmNtCSDVersion) : 1
Build string (NtBuildLab) : 7601.17514.amd64fre.win7sp1_rtm.
PsActiveProcessHead : 0xffffffff8000283ab90 (37 processes)
PsLoadedModuleList : 0xffffffff80002858e90 (139 modules)
KernelBase : 0xffffffff80002613000 (Matches MZ: True)
Major (OptionalHeader) : 6
Minor (OptionalHeader) : 1
KPCR : 0xffffffff80002805d00 (CPU 0)
```

Vemos que el ‘Build String’ es ‘7601.17514.amd64fre.win7sp1\_rtm.’, así que lo abriremos con el *profile* de ‘Win7SP1x64’.

Miramos los procesos en memoria con el plugin ‘pstree’:

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                               Pid    PPid    Thds    Hnds    Time
-----
0xfffffa8003805460:explorer.exe     1996   1956    36      877    2018-03-12 20:33:29 UTC+0000
. 0xfffffa80038d37d0:VBoxTray.exe   1792   1996    15      155    2018-03-12 20:33:29 UTC+0000
. 0xfffffa8003be0600:DumpIt.exe     1208   1996     6       93    2018-03-12 20:35:18 UTC+0000
. 0xfffffa80018cc060:wininit.exe     412    368     3       75    2018-03-12 20:33:16 UTC+0000
. 0xfffffa800341c270:lsass.exe       528    412     8      700    2018-03-12 20:33:18 UTC+0000
. 0xfffffa80033a46e0:lsm.exe        536    412    10     144    2018-03-12 20:33:18 UTC+0000
. 0xfffffa800337fb30:services.exe   508    412    10     186    2018-03-12 20:33:16 UTC+0000
.. 0xfffffa800350bb30:svchost.exe    916    508    29     545    2018-03-12 20:33:19 UTC+0000
... 0xfffffa80036fb060:dwm.exe       1976   916     4       71    2018-03-12 20:33:29 UTC+0000
.. 0xfffffa80037e0a70:taskhost.exe   1924   508    11     172    2018-03-12 20:33:29 UTC+0000
.. 0xfffffa80034d1740:svchost.exe    804    508    22     508    2018-03-12 20:33:19 UTC+0000
... 0xfffffa8003556b30:audiodg.exe   316    804     7     125    2018-03-12 20:33:19 UTC+0000
.. 0xfffffa8003c54060:mscorsvw.exe   2972   508     5       60    2018-03-12 20:35:38 UTC+0000
.. 0xfffffa800382c510:SearchIndexer. 2256   508    12     601    2018-03-12 20:33:35 UTC+0000
... 0xfffffa800395f7d0:SearchFilterHo 2344   2256     4       77    2018-03-12 20:33:36 UTC+0000
... 0xfffffa80039482a0:SearchProtocol 2324   2256     7     224    2018-03-12 20:33:36 UTC+0000
.. 0xfffffa8003963b30:wmpnetwk.exe   2448   508    15     427    2018-03-12 20:33:37 UTC+0000
.. 0xfffffa8003494060:VBoxService.ex 700    508    13     118    2018-03-12 20:33:19 UTC+0000
.. 0xfffffa800352ab30:svchost.exe    960    508    40     887    2018-03-12 20:33:19 UTC+0000
... 0xfffffa8003806b30:taskeng.exe    1984   960     6      82    2018-03-12 20:33:29 UTC+0000
.. 0xfffffa8003acb4a0:svchost.exe    2644   508    10     354    2018-03-12 20:33:38 UTC+0000
.. 0xfffffa80035924a0:svchost.exe    868    508    19     469    2018-03-12 20:33:20 UTC+0000
.. 0xfffffa80035d1b30:spoolsv.exe    1232   508    15     290    2018-03-12 20:33:20 UTC+0000
.. 0xfffffa80036b3060:svchost.exe    1380   508    22     292    2018-03-12 20:33:22 UTC+0000
.. 0xfffffa80035c6740:svchost.exe    1132   508    17     462    2018-03-12 20:33:20 UTC+0000
.. 0xfffffa80034a85f0:svchost.exe    752    508     8     276    2018-03-12 20:33:19 UTC+0000
.. 0xfffffa80036205f0:svchost.exe    1268   508    21     319    2018-03-12 20:33:20 UTC+0000
.. 0xfffffa800346f4b0:svchost.exe    636    508    10     358    2018-03-12 20:33:19 UTC+0000
... 0xfffffa8003bbcab0:WmiPrvSE.exe   2828   636     8     123    2018-03-12 20:34:10 UTC+0000
... 0xfffffa80037e7630:dllhost.exe    3020   636    10     167    2018-03-12 20:33:58 UTC+0000
... 0xfffffa8003b136b0:WmiPrvSE.exe   2780   636     8     117    2018-03-12 20:33:38 UTC+0000
0xfffffa8003415060:csrss.exe       376    368     9     426    2018-03-12 20:33:16 UTC+0000
0xfffffa80018c5040:System           4       0     91    512    2018-03-12 20:33:05 UTC+0000
. 0xfffffa800295cb30:smss.exe        268     4     2      29    2018-03-12 20:33:06 UTC+0000
0xfffffa80018cb5b0:csrss.exe       424    404     7     209    2018-03-12 20:33:16 UTC+0000
. 0xfffffa8003754060:conhost.exe    1280   424     2      56    2018-03-12 20:35:18 UTC+0000
0xfffffa800337c330:winlogon.exe     464    404     6     114    2018-03-12 20:33:16 UTC+0000
>
```

Y también un ‘psscan’ para ver los que había antes en ejecución:

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Name                               PID    PPID    PDB                               Time created          Time exited
-----
0x000000007d9b6910 DumpIt.exe                       2672   1996   0x000000006e5ec000 2018-03-12 20:34:05 UTC+0000 2018-03-12 20:34:53 UTC+0000
0x000000007d9b6910 DumpIt.exe                       2672   1996   0x000000006e5ec000 2018-03-12 20:34:05 UTC+0000 2018-03-12 20:34:53 UTC+0000
0x000000007d9f4060 mscorsvw.exe                     2972   508    0x0000000062479000 2018-03-12 20:35:38 UTC+0000
0x000000007dae7040 System                               4       0   0x0000000001870000 2018-03-12 20:33:05 UTC+0000
0x000000007dae5b0 csrss.exe                        424    404    0x000000002c0ef000 2018-03-12 20:33:16 UTC+0000
```

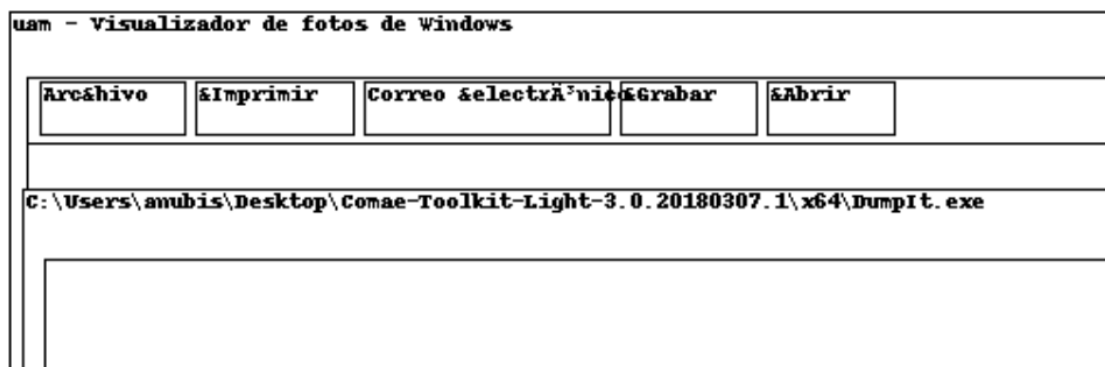
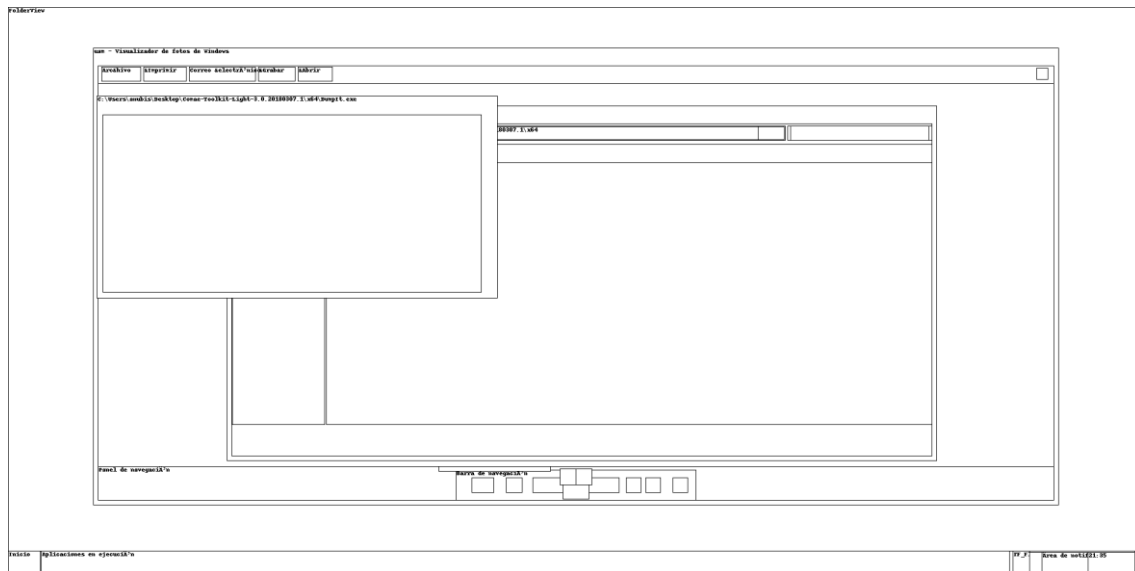
Detectamos que se había ejecutado anteriormente dos veces el proceso DumpIt.exe

Analizando los procesos no se detecta ningún proceso que llame la atención.

Intentaremos obtener una reconstrucción del escritorio:

```
>volatility -f morfeo.dmp --profile=Win7SP1x64 screenshot -D /output/
```

En la reconstrucción observamos que tiene abierto el “*Visualizador de fotos de Windows*” y la foto de nombre “*uam*”, así que ya sabemos por dónde tirar:



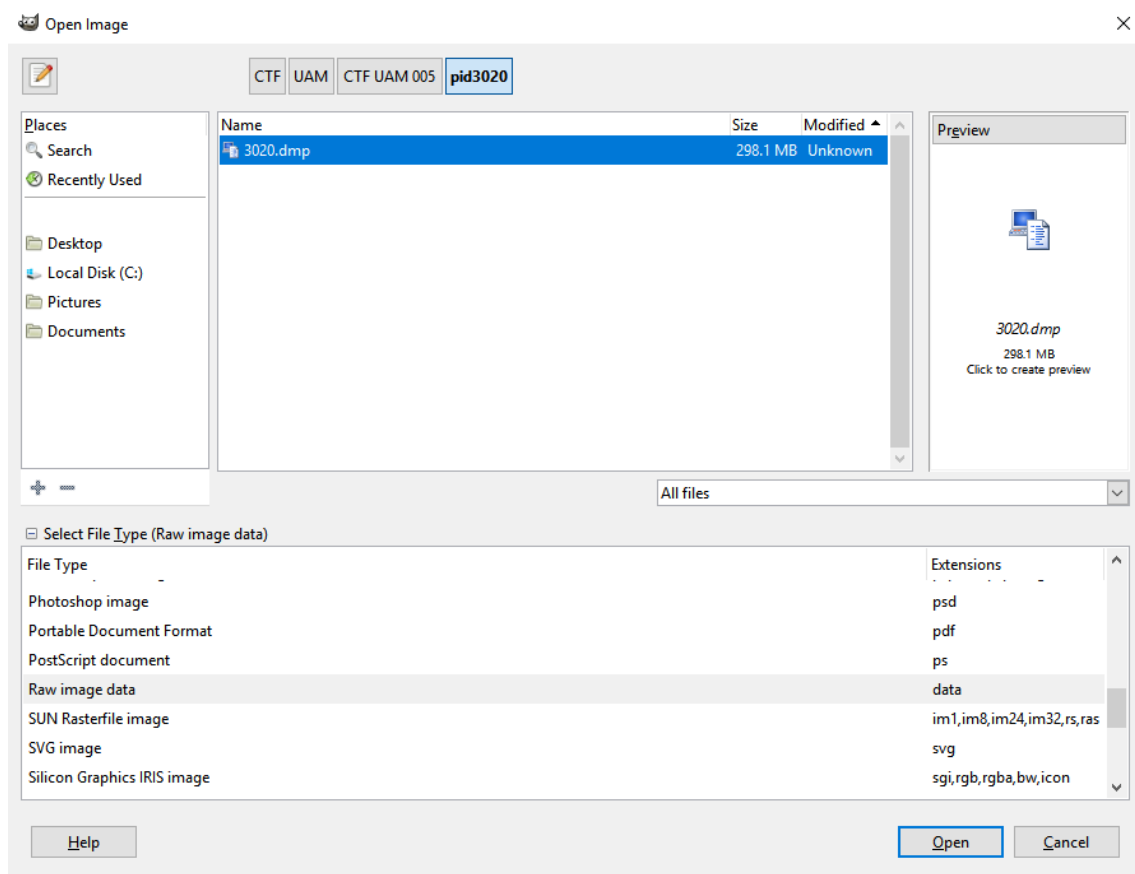
Vamos a intentar reconstruir esta imagen, sabiendo que el proceso es ‘*dllhost.exe*’, así que obtenemos su PID (3020):

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 pslist --name dllhost.exe
Volatility Foundation Volatility Framework 2.6
Offset(V)      Name                PID    PPID    Thds    Hnds    Sess    Wow64    Start
-----
0xffffffffa80037e7630 dllhost.exe          3020    636     10     167     1      0 2018-03-12 20:33:58 UTC+0000
```

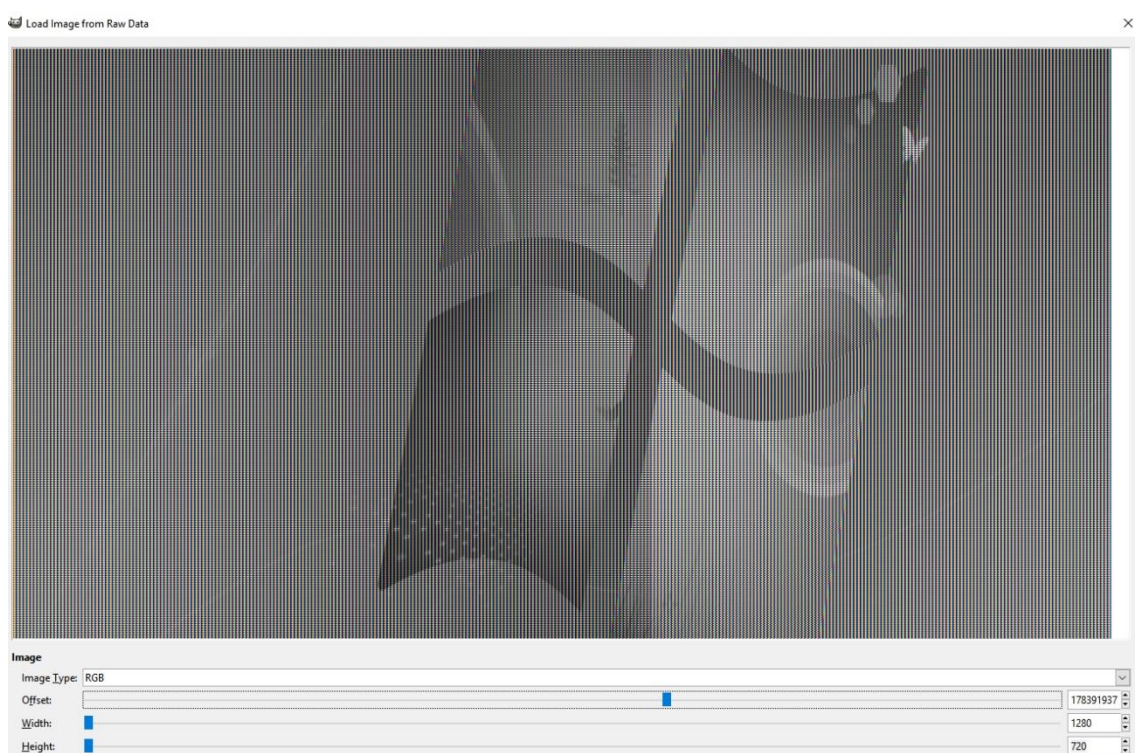
Volcamos todos los datos del proceso para su posterior análisis

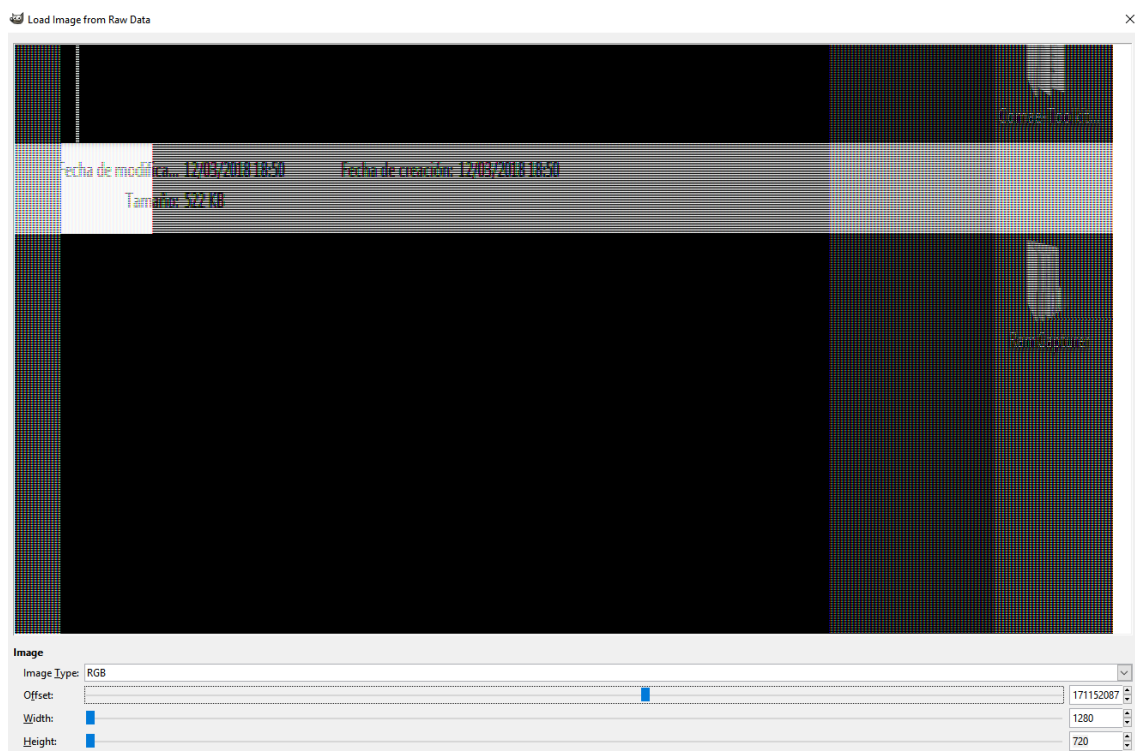
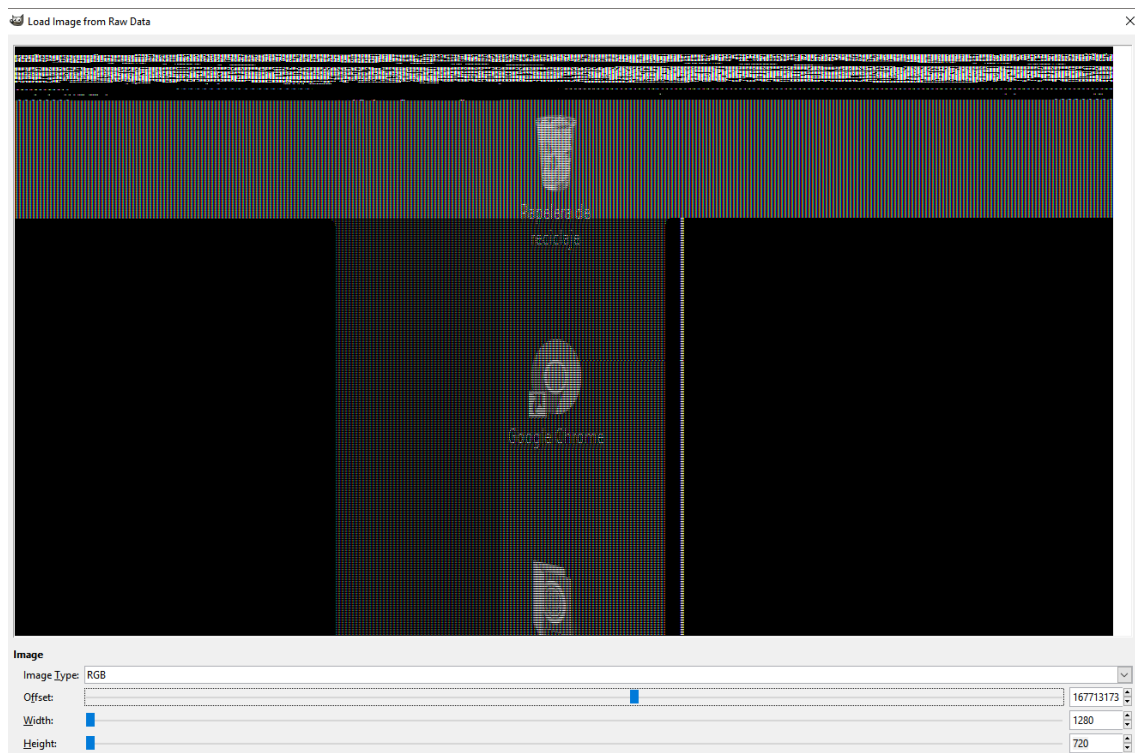
```
>volatility -f morfeo.dmp --profile=Win7SP1x64 memdump -p 3020 --dump ./pid3020/
Volatility Foundation Volatility Framework 2.6
*****
Writing dllhost.exe [ 3020] to 3020.dmp
```

Obtenido el Dump del proceso, intentaremos regenerar con el Gimp el escritorio. Para eso abrimos el fichero ‘*.dmp*’ generado como imagen Raw. Ponemos la resolución a 1280 x 720 y vamos mirando a ver si podemos encontrar un ‘*screenshot*’ de la pantalla:



Solamente podemos regenerar un par de imágenes con el fondo de pantalla y algunos iconos, pero nada que nos sirva:







Vamos a mirar si hay algo en el portapapeles. La única sesión que tiene algo es la 1, pero tampoco sabemos avanzar a partir de aquí ya que no sabemos su formato ('*Unknow*')

```
>volatility -f morfeo.dmp --profile=Win7SP1x64 wndscan
Volatility Foundation Volatility Framework 2.6
*****
WindowStation: 0x7e597d30, Name: WinSta0, Next: 0x0
SessionId: 1, AtomTable: 0xfffff8a005d4e110, Interactive: True
Desktops: Default, Disconnect, Winlogon
ptiDrawingClipboard: pid - tid -
spwndClipOpen: 0x0, spwndClipViewer: 0x0
cNumClipFormats: 5, iClipSerialNumber: 2
pClipBase: 0xfffff900c1b81da0, Formats: Unknown choice 3248575072,Unknown
choice 0,Unknown choice 3261317800,Unknown choice 3222142992,Unknown
choice 5000
*****
```

Los siguientes procesos también están involucrados en las tareas de copiar y pegar:

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 wintree | grep
CLIPBRDWNDCLASS
Volatility Foundation Volatility Framework 2.6
.#10084 explorer.exe:1996 CLIPBRDWNDCLASS
.#10122 explorer.exe:1996 CLIPBRDWNDCLASS
.#1013c VBoxTray.exe:1792 CLIPBRDWNDCLASS
.#10206 explorer.exe:1996 CLIPBRDWNDCLASS
.#10084 explorer.exe:1996 CLIPBRDWNDCLASS
.#10122 explorer.exe:1996 CLIPBRDWNDCLASS
.#1013c VBoxTray.exe:1792 CLIPBRDWNDCLASS
.#10206 explorer.exe:1996 CLIPBRDWNDCLASS
```

Así que callejón sin salida. Volvemos al PID 3020 (dllhost.exe) y observamos que al realizar la opción '*pstree*', éste cuelga del proceso explorer.exe (PID 1966).

Realizamos el mismo procedimiento anterior para ver si podemos extraer un screenshot para el proceso explorer.exe pero obtenemos el mismo resultado.

Procederemos al volcado de los ficheros cacheados en memoria del PID 1966 (explorer.exe) a ver si obtenemos alguna pista. Por cada fichero, se extrae la sección de datos del archivo, la sección de imagen y la ‘SharedCacheMap’.

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 dumpfiles -n -p 1966 -D ./pid1966/
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0xffffffff8002db6210 1966 \Device\HarddiskVolume2\Windows\es-ES\explorer.exe.mui
DataSectionObject 0xffffffff8002db6950 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\setupapi.dll.mui
DataSectionObject 0xffffffff800381b8d0 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\shell32.dll.mui
DataSectionObject 0xffffffff80038a36a0 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\msctf.dll.mui
DataSectionObject 0xffffffff800384cdd0 1966 \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
SharedCacheMap 0xffffffff800384cdd0 1966 \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
DataSectionObject 0xffffffff80037d92d0 1966 \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls.resources_6595b64144ccf1df_6.0.7600.16385_es-es_103af8cc43d0a688\comctl32.dll.mui
DataSectionObject 0xffffffff80038ac920 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\msutb.dll.mui
DataSectionObject 0xffffffff80038c5b40 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\explorerframe.dll.mui
DataSectionObject 0xffffffff80038c68b0 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\authui.dll.mui
DataSectionObject 0xffffffff80038d0530 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\propsys.dll.mui
DataSectionObject 0xffffffff8002dc8070 1966 \Device\HarddiskVolume2\Users\anubis\AppData\Local\Microsoft\Windows\Explorer\thumbcache_100.db
DataSectionObject 0xffffffff8002c4ed10 1966 \Device\HarddiskVolume2\Users\anubis\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
DataSectionObject 0xffffffff8003bb7f20 1966 \Device\HarddiskVolume2\Users\anubis\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
DataSectionObject 0xffffffff8003201810 1966 \Device\HarddiskVolume2\Users\anubis\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
DataSectionObject 0xffffffff80034cf070 1966 \Device\HarddiskVolume2
DataSectionObject 0xffffffff80037df340 1966 \Device\HarddiskVolume2\Users\anubis\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db
DataSectionObject 0xffffffff8003c2b330 1966 \Device\HarddiskVolume2\Windows\System32\es-ES\explorer.dll.mui
```

Revisando algunos de ellos vemos que hay ficheros del tipo *thumbcache* (que al abrirlos solo nos muestran iconos), y también vemos algún *index.dat*. Al abrirlo nos muestra información de la ubicación de un fichero ‘*uam.jpg*’ ubicado en el escritorio del usuario *anubis*:

```
853 00004f80: efbe adde efbe adde 5552 4c20 0200 0000 50a8 afa2 2aba d301 .....URL.....P.....*...
854 00004ff8: efbe adde efbe adde 5552 4c20 0200 0000 50a8 afa2 2aba d301 .....URL.....P.....*...
855 00005010: 50a8 afa2 2aba d301 874c 558e 0000 0000 0000 0000 0000 0000 :P.....*...LU.....
856 00005028: 0000 0000 0000 0000 6000 0000 6800 0000 fe00 1010 0000 0000 :.....~.h.....
857 00005040: 0100 2000 a000 0000 0000 1400 0000 0000 0000 0000 6c4c 558e 0100 0000 :.....LLU.....
858 00005058: 0000 0000 0000 0000 0000 0000 efbe adde 5669 7369 7465 643a :.....Visited:
859 00005070: 2061 6e75 6269 7340 6669 6c65 3a2f 2f2f 433a 2f55 7365 7273 : anubis@file:///C:/Users
860 00005088: 2f61 6e75 6269 732f 4465 736b 746f 702f 7561 6d2e 6a70 6700 :/anubis/Desktop/uam.jpg.
861 000050a0: 1000 0200 0000 0010 0000 0000 0100 0000 0000 0000 efbe adde :.....
862 000050b8: efbe adde efbe adde efbe adde efbe adde efbe adde efbe adde :.....
863 000050d0: efbe adde efbe adde efbe adde efbe adde efbe adde efbe adde :.....
864 000050e8: efbe adde efbe adde efbe adde efbe adde efbe adde efbe adde :.....
865 00005100: 5552 4c20 0200 0000 60bb 11a8 46b9 d301 60bb 11a8 46b9 d301 :URL.....~.F.....F...
866 00005118: 864c d774 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 :.L.t.....
867 00005130: 6000 0000 6800 0000 fe00 1010 0000 0000 0100 2000 ac00 0000 :~.h.....
868 00005148: 1400 0000 0000 0000 6b4c d774 0200 0000 0000 0000 0000 0000 :.....kL.t.....
869 00005160: 0000 0000 efbe adde 5669 7369 7465 643a 2061 6e75 6269 7340 :.....Visited: anubis@
870 00005178: 6669 6c65 3a2f 2f2f 433a 2f55 7365 7273 2f61 6e75 6269 732f :file:///C:/Users/anubis/
871 00005190: 446f 776e 6c6f 6164 732f 5261 6d43 6170 7475 7265 722e 7a69 :Downloads/RamCaptor.zi
872 000051a8: 7000 adde 1000 0200 0000 0010 0000 0000 0200 0000 0000 0000 :p.....
873 000051c0: efbe adde efbe adde efbe adde efbe adde efbe adde efbe adde :.....
874 000051d8: efbe adde efbe adde efbe adde efbe adde efbe adde efbe adde :.....
875 000051f0: efbe adde efbe adde efbe adde efbe adde 5552 4c20 0200 0000 :.....URL.....
876 00005208: 5016 4673 41ba d301 5016 4673 41ba d301 874c 40a4 0000 0000 :P.FsA...P.FsA...L@.....
877 00005220: 0000 0000 0000 0000 0000 0000 0000 0000 6000 0000 6800 0000 :.....~.h.....
878 00005238: fe00 1010 0000 0000 0100 2000 a000 0000 1400 0000 0000 0000 :.....
879 00005250: 6c4c 40a4 0200 0000 0000 0000 0000 0000 0000 0000 efbe adde :LL@.....
880 00005268: 5669 7369 7465 643a 2061 6e75 6269 7340 6669 6c65 3a2f 2f2f :Visited: anubis@file:///
881 00005280: 433a 2f55 7365 7273 2f61 6e75 6269 732f 4465 736b 746f 702f :C:/Users/anubis/Desktop/
882 00005298: 7561 6d2e 6a70 6700 1000 0200 0000 0010 0000 0000 0200 0000 :uam.jpg.....
883 000052b0: 0000 0000 efbe adde efbe adde efbe adde efbe adde efbe adde :.....
```

Así que buscamos ficheros con extensión ‘.jpg’ o nombre ‘uam’:

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 filescan | grep jpg
Volatility Foundation Volatility Framework 2.6
0x000000007ddb0540 16 0 -W-r-- \Device\HarddiskVolume2\Users\anubis\Desktop\uam.jpg.jpgVirtualBox Dropped Files\2018-03-12T20_33_51.765201500Z\uam (2).jpg
0x000000007dedea70 11 0 R--r-- \Device\HarddiskVolume2\Users\anubis\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg
0x000000007df0b350 16 0 R--r-- \Device\HarddiskVolume2\Users\anubis\Desktop\uam.jpg
0x000000007e1c2940 16 0 -W---- \Device\HarddiskVolume2\Recycle.Bin\5-1-5-21-3107480389-3703109444-792598018-1001\SIGKW\FUM.jpg
> volatility -f morfeo.dmp --profile=Win7SP1x64 filescan | grep uam
Volatility Foundation Volatility Framework 2.6
0x000000007ddb0540 16 0 -W-r-- \Device\HarddiskVolume2\Users\anubis\Desktop\uam.jpg.jpgVirtualBox Dropped Files\2018-03-12T20_33_51.765201500Z\uam (2).jpg
0x000000007ddc5070 2 0 RW-rw- \Device\HarddiskVolume2\Users\anubis\AppData\Roaming\Microsoft\Windows\Recent\uam (2).lnk
0x000000007df0b350 16 0 R--r-- \Device\HarddiskVolume2\Users\anubis\Desktop\uam.jpg
```

Ya parece que lleguemos al final. Vemos que hay un fichero 'uam.jpg' en el escritorio y otro fichero 'uam (2).lnk' que es un acceso directo.

Intentamos extraerlos, pero no extrae nada:

```
>volatility -f morfeo.dmp --profile=Win7SP1x64 dumpfiles -r jpg$ -i -n -u  
-S resumen.txt -D ./
```

Intentamos poniendo el offset físico:

```
> volatility -f morfeo.dmp --profile=Win7SP1x64 dumpfiles -Q 0x000000007e1c2940 -n -u -S ./dumpfiles/resumen.txt -D ./du  
mpfiles/  
Volatility Foundation Volatility Framework 2.6  
DataSectionObject 0x7e1c2940 None \Device\HarddiskVolume2\Recycle.Bin\S-1-5-21-3107480389-3703109444-792598018-1001  
\$IGKWFUM.jpg
```

Tampoco conseguimos descargar el fichero para poderlo abrir:

Name	Date modified	Type	Size
file.None.0xfffffa8003520420.\$IGKWFUM.jpg.dat	21/03/2018 14:29	DAT File	4 KB
resumen.txt	21/03/2018 14:29	Text Document	5 KB

resumen.txt - Notepad

File Edit Format View Help

```
{ "name": "\\Device\\HarddiskVolume2\\$Recycle.Bin\\S-1-5-21-3107480389-3703109444-792598018-1001\\$IGKWFUM.jpg",  
  "ofpath": ".\\dumpfiles\\file.None.0xfffffa8003520420.$IGKWFUM.jpg.dat", "pid":  
  4096, [8192, 4096], [12288, 4096], [16384, 4096], [20480, 4096], [24576, 4096], [28672, 4096], [32768, 4096], [36864, 4096], [40960, 4096], [45056, 4096], [49152, 4096], [53248, 4096], [57344, 4096], [61440, 4096], [65536, 4096], [69632, 4096], [73728, 4096], [77824, 4096], [81920, 4096], [86016, 4096], [90112, 4096], [94208, 4096], [98304, 4096], [102400, 4096], [106496, 4096], [110592, 4096], [114688, 4096], [118784, 4096], [122880, 4096], [126976, 4096], [131072, 4096], [135168, 4096], [139264, 4096], [143360, 4096], [147456, 4096], [151552, 4096], [155648, 4096], [159744, 4096], [163840, 4096], [167936, 4096], [172032, 4096], [176128, 4096], [180224, 4096], [184320, 4096], [188416, 4096], [192512, 4096], [196608, 4096], [200704, 4096], [204800, 4096], [208896, 4096], [212992, 4096], [217088, 4096], [221184, 4096], [225280, 4096], [229376, 4096], [233472, 4096], [237568, 4096], [241664, 4096], [245760, 4096], [249856, 4096], [253952, 4096], [258048, 4096], [262144, 4096], [266240, 4096], [270336, 4096], [274432, 4096], [278528, 4096], [282624, 4096], [286720, 4096], [290816, 4096], [294912, 4096], [299008, 4096], [303104, 4096], [307200, 4096], [311296, 4096], [315392, 4096], [319488, 4096], [323584, 4096], [327680, 4096], [331776, 4096], [335872, 4096], [339968, 4096], [344064, 4096], [348160, 4096], [352256, 4096], [356352, 4096], [360448, 4096], [364544, 4096], [368640, 4096], [372736, 4096], [376832, 4096], [380928, 4096], [385024, 4096], [389120, 4096], [393216, 4096], [397312, 4096], [401408, 4096], [405504, 4096], [409600, 4096], [413696, 4096], [417792, 4096], [421888, 4096], [425984, 4096], [430080, 4096], [434176, 4096], [438272, 4096], [442368, 4096], [446464, 4096], [450560, 4096], [454656, 4096], [458752, 4096], [462848, 4096], [466944, 4096], [471040, 4096], [475136, 4096], [479232, 4096], [483328, 4096], [487424, 4096], [491520, 4096], [495616, 4096], [499712, 4096], [503808, 4096], [507904, 4096], [512000, 4096], [516096, 4096], [520192, 4096], [524288, 4096], [528384, 4096], [532480, 4096], [536576, 4096], [540672, 4096], [544768, 4096], [548864, 4096], [552960, 4096], [557056, 4096], [561152, 4096], [565248, 4096], [569344, 4096], [573440, 4096], [577536, 4096], [581632, 4096], [585728, 4096], [589824, 4096], [593920, 4096], [598016, 4096], [602112, 4096], [606208, 4096], [610304, 4096], [614400, 4096], [618496, 4096], [622592, 4096], [626688, 4096], [630784, 4096], [634880, 4096], [638976, 4096], [643072, 4096], [647168, 4096], [651264, 4096], [655360, 4096], [659456, 4096], [663552, 4096], [667648, 4096], [671744, 4096], [675840, 4096], [679936, 4096], [684032, 4096], [688128, 4096], [692224, 4096], [696320, 4096], [700416, 4096], [704512, 4096], [708608, 4096], [712704, 4096], [716800, 4096], [720896, 4096], [724992, 4096], [729088, 4096], [733184, 4096], [737280, 4096], [741376, 4096], [745472, 4096], [749568, 4096], [753664, 4096], [757760, 4096], [761856, 4096], [765952, 4096], [770048, 4096], [774144, 4096], [778240, 4096], [782336, 4096], [786432, 4096], [790528, 4096], [794624, 4096], [798720, 4096], [802816, 4096], [806912, 4096], [811008, 4096], [815104, 4096], [819200, 4096], [823296, 4096], [827392, 4096], [831488, 4096], [835584, 4096], [839680, 4096], [843776, 4096], [847872, 4096], [851968, 4096], [856064, 4096], [860160, 4096], [864256, 4096], [868352, 4096], [872448, 4096], [876544, 4096], [880640, 4096], [884736, 4096], [888832, 4096], [892928, 4096], [897024, 4096], [901120, 4096], [905216, 4096], [909312, 4096], [913408, 4096], [917504, 4096], [921600, 4096], [925696, 4096], [929792, 4096], [933888, 4096], [937984, 4096], [942080, 4096], [946176, 4096], [950272, 4096], [954368, 4096], [958464, 4096], [962560, 4096], [966656, 4096], [970752, 4096], [974848, 4096], [978944, 4096], [983040, 4096], [987136, 4096], [991232, 4096], [995328, 4096], [999424, 4096], [1003520, 4096], [1007616, 4096], [1011712, 4096], [1015808, 4096], [1019904, 4096], [1024000, 4096], [1028096, 4096], [1032192, 4096], [1036288, 4096], [1040384, 4096], [1044480, 4096], [1048576, 4096], [1052672, 4096], [1056768, 4096], [1060864, 4096], [1064960, 4096], [1069056, 4096], [1073152, 4096], [1077248, 4096], [1081344, 4096], [1085440, 4096], [1089536, 4096], [1093632, 4096], [1097728, 4096], [1101824, 4096], [1105920, 4096], [1110016, 4096], [1114112, 4096], [1118208, 4096], [1122304, 4096], [1126400, 4096], [1130496, 4096], [1134592, 4096], [1138688, 4096], [1142784, 4096], [1146880, 4096], [1150976, 4096], [1155072, 4096], [1159168, 4096], [1163264, 4096], [1167360, 4096], [1171456, 4096], [1175552, 4096], [1179648, 4096], [1183744, 4096], [1187840, 4096], [1191936, 4096], [1196032, 4096], [1200128, 4096], [1204224, 4096], [1208320, 4096], [1212416, 4096], [1216512, 4096], [1220608, 4096], [1224704, 4096], [1228800, 4096], [1232896, 4096], [1236992, 4096], [1241088, 4096], [1245184, 4096], [1249280, 4096], [1253376, 4096], [1257472, 4096], [1261568, 4096], [1265664, 4096], [1269760, 4096], [1273856, 4096], [1277952, 4096], [1282048, 4096], [1286144, 4096], [1290240, 4096], [1294336, 4096], [1298432, 4096], [1302528, 4096], [1306624, 4096], [1310720, 4096], [1314816, 4096], [1318912, 4096], [1323008, 4096], [1327104, 4096], [1331200, 4096], [1335296, 4096], [1339392, 4096], [1343488, 4096], [1347584, 4096], [1351680, 4096], [1355776, 4096], [1359872, 4096], [1363968, 4096], [1368064, 4096], [1372160, 4096], [1376256, 4096], [1380352, 4096], [1384448, 4096], [1388544, 4096], [1392640, 4096], [1396736, 4096], [1400832, 4096], [1404928, 4096], [1409024, 4096], [1413120, 4096], [1417216, 4096], [1421312, 4096], [1425408, 4096], [1429504, 4096], [1433600, 4096], [1437696, 4096], [1441792, 4096], [1445888, 4096], [1449984, 4096], [1454080, 4096], [1458176, 4096], [1462272, 4096], [1466368, 4096], [1470464, 4096], [1474560, 4096], [1478656, 4096], [1482752, 4096], [1486848, 4096], [1490944, 4096], [1495040, 4096], [1499136, 4096], [1503232, 4096], [1507328, 4096], [1511424, 4096], [1515520, 4096], [1519616, 4096], [1523712, 4096], [1527808, 4096], [1531904, 4096], [1536000, 4096], [1540096, 4096], [1544192, 4096], [1548288, 4096], [1552384, 4096], [1556480, 4096], [1560576, 4096], [1564672, 4096], [1568768, 4096], [1572864, 4096], [1576960, 4096], [1581056, 4096], [1585152, 4096], [1589248, 4096], [1593344, 4096], [1597440, 4096], [1601536, 4096], [1605632, 4096], [1609728, 4096], [1613824, 4096], [1617920, 4096], [1622016, 4096], [1626112, 4096], [1630208, 4096], [1634304, 4096], [1638400, 4096], [1642496, 4096], [1646592, 4096], [1650688, 4096], [1654784, 4096], [1658880, 4096], [1662976, 4096], [1667072, 4096], [1671168, 4096], [1675264, 4096], [1679360, 4096], [1683456, 4096], [1687552, 4096], [1691648, 4096], [1695744, 4096], [1699840, 4096], [1703936, 4096], [1708032, 4096], [1712128, 4096], [1716224, 4096], [1720320, 4096], [1724416, 4096], [1728512, 4096], [1732608, 4096], [1736704, 4096], [1740800, 4096], [1744896, 4096], [1748992, 4096], [1753088, 4096], [1757184, 4096], [1761280, 4096], [1765376, 4096], [1769472, 4096], [1773568, 4096], [1777664, 4096], [1781760, 4096], [1785856, 4096], [1789952, 4096], [1794048, 4096], [1798144, 4096], [1802240, 4096], [1806336, 4096], [1810432, 4096], [1814528, 4096], [1818624, 4096], [1822720, 4096], [1826816, 4096], [1830912, 4096], [1835008, 4096], [1839104, 4096], [1843200, 4096], [1847296, 4096], [1851392, 4096], [1855488, 4096], [1859584, 4096], [1863680, 4096], [1867776, 4096], [1871872, 4096], [1875968, 4096], [1880064, 4096], [1884160, 4096], [1888256, 4096], [1892352, 4096], [1896448, 4096], [1900544, 4096], [1904640, 4096], [1908736, 4096], [1912832, 4096], [1916928, 4096], [1921024, 4096], [1925120, 4096], [1929216, 4096], [1933312, 4096], [1937408, 4096], [1941504, 4096], [1945600, 4096], [1949696, 4096], [1953792, 4096], [1957888, 4096], [1961984, 4096], [1966080, 4096], [1970176, 4096], [1974272, 4096], [1978368, 4096], [1982464, 4096], [1986560, 4096], [1990656, 4096], [1994752, 4096], [1998848, 4096], [2002944, 4096], [2007040, 4096], [2011136, 4096], [2015232, 4096], [2019328, 4096], [2023424, 4096], [2027520, 4096], [2031616, 4096], [2035712, 4096], [2039808, 4096], [2043904, 4096], [2048000, 4096], [2052096, 4096], [2056192, 4096], [2060288, 4096], [2064384, 4096], [2068480, 4096], [2072576, 4096], [2076672, 4096], [2080768, 4096], [2084864, 4096], [2088960, 4096], [2093056, 4096], [2097152, 4096], [2101248, 4096], [2105344, 4096], [2109440, 4096], [2113536, 4096], [2117632, 4096], [2121728, 4096], [2125824, 4096], [2129920, 4096], [2134016, 4096], [2138112, 4096], [2142208, 4096], [2146304, 4096], [2150400, 4096], [2154496, 4096], [2158592, 4096], [2162688, 4096], [2166784, 4096], [2170880, 4096], [2174976, 4096], [2179072, 4096], [2183168, 4096], [2187264, 4096], [2191360, 4096], [2195456, 4096], [2199552, 4096], [2203648, 4096], [2207744, 4096], [2211840, 4096], [2215936, 4096], [2220032, 4096], [2224128, 4096], [2228224, 4096], [2232320, 4096], [2236416, 4096], [2240512, 4096], [2244608, 4096], [2248704, 4096], [2252800, 4096], [2256896, 4096], [2260992, 4096], [2265088, 4096], [2269184, 4096], [2273280, 4096], [2277376, 4096], [2281472, 4096], [2285568, 4096], [2289664, 4096], [2293760, 4096], [2297856, 4096], [2301952, 4096], [2306048, 4096], [2310144, 4096], [2314240, 4096], [2318336, 4096], [2322432, 4096], [2326528, 4096], [2330624, 4096], [2334720, 4096], [2338816, 4096], [2342912, 4096], [2347008, 4096], [2351104, 4096], [2355200, 4096], [2359296, 4096], [2363392, 4096], [2367488, 4096], [2371584, 4096], [2375680, 4096], [2379776, 4096], [2383872, 4096], [2387968, 4096], [2392064, 4096], [2396160, 4096], [2400256, 4096], [2404352, 4096], [2408448, 4096], [2412544, 4096], [2416640, 4096], [2420736, 4096], [2424832, 4096], [2428928, 4096], [2433024, 4096], [2437120, 4096], [2441216, 4096], [2445312, 4096], [2449408, 4096], [2453504, 4096], [2457600, 4096], [2461696, 4096], [2465792, 4096], [2469888, 4096], [2473984, 4096], [2478080, 4096], [2482176, 4096], [2486272, 4096], [2490368, 4096], [2494464, 4096], [2498560, 4096], [2502656, 4096], [2506752, 4096], [2510848, 4096], [2514944, 4096], [2519040, 4096], [2523136, 4096], [2527232, 4096], [2531328, 4096], [2535424, 4096], [2539520, 4096], [2543616, 4096], [2547712, 4096], [2551808, 4096], [2555904, 4096], [2560000, 4096], [2564096, 4096], [2568192, 4096], [2572288, 4096], [2576384, 4096], [2580480, 4096], [2584576, 4096], [2588672, 4096], [2592768, 4096], [2596864, 4096], [2600960, 4096], [2605056, 4096], [2609152, 4096], [2613248, 4096], [2617344, 4096], [2621440, 4096], [2625536, 4096], [2629632, 4096], [2633728, 4096], [2637824, 4096], [2641920, 4096], [2646016, 4096], [2650112, 4096], [2654208, 4096], [2658304, 4096], [2662400, 4096], [2666496, 4096], [2670592, 4096], [2674688, 4096], [2678784, 4096], [2682880, 4096], [2686976, 4096], [2691072, 4096], [2695168, 4096], [2699264, 4096], [2703360, 4096], [2707456, 4096], [2711552, 4096], [2715648, 4096], [2719744, 4096], [2723840, 4096], [2727936, 4096], [2732032, 4096], [2736128, 4096], [2740224, 4096], [2744320, 4096], [2748416, 4096], [2752512, 4096], [2756608, 4096], [2760704, 4096], [2764800, 4096], [2768896, 4096], [2772992, 4096], [2777088, 4096], [2781184, 4096], [2785280, 4096], [2789376, 4096], [2793472, 4096], [2797568, 4096], [2801664, 4096], [2805760, 4096], [2809856, 4096], [2813952, 4096], [2818048, 4096], [2822144, 4096], [2826240, 4096], [2830336, 4096], [2834432, 4096], [2838528, 4096], [2842624, 4096], [2846720, 4096], [2850816, 4096], [2854912, 4096], [2859008, 4096], [2863104, 4096], [2867200, 4096], [2871296, 4096], [2875392, 4096], [2879488, 4096], [2883584, 4096], [2887680, 4096], [2891776, 4096], [2895872, 4096], [2900000, 4096], [2904096, 4096], [2908192, 4096], [2912288, 4096], [2916384, 4096], [2920480, 4096], [2924576, 4096], [2928672, 4096], [2932768, 4096], [2936864, 4096], [2940960, 4096], [2945056, 4096], [2949152, 4096], [2953248, 4096], [2957344, 4096], [2961440, 4096], [2965536, 4096], [2969632, 4096], [2973728, 4096], [2977824, 4096], [2981920, 4096], [2986016, 4096], [2990112, 4096], [2994208, 4096], [2998304, 4096], [3002400, 4096], [3006496, 4096], [3010592, 4096], [3014688, 4096], [3018784, 4096], [3022880, 4096], [3026976, 4096], [3031072, 4096], [3035168, 4096], [3039264, 4096], [3043360, 4096], [3047456, 4096], [3051552, 4096], [3055648, 4096], [3059744, 4096], [3063840, 4096], [3067936, 4096], [3072032, 4096], [3076128, 4096], [3080224, 4096], [3084320, 4096], [3088416, 4096], [3092512, 4096], [3096608, 4096], [3100704, 4096], [3104800, 4096], [3108896, 4096], [3112992, 4096], [3117088, 4096], [3121184, 4096], [3125280, 4096], [3129376, 4096], [3133472, 4096], [3137568, 4096], [3141664, 4096], [3145760, 4096], [3149856, 4096], [3153952, 4096], [3158048, 4096], [3162144, 4096], [3166240, 4096], [3170336, 4096], [3174432, 4096], [3178528, 4096], [3182624, 4096], [3186720, 4096], [3190816, 4096], [3194912, 4096], [3199008, 4096], [3203104, 4096], [3207200, 4096], [3211296, 4096], [3215392, 4096], [3219488, 4096], [3223584, 4096], [3227680, 4096], [3231776, 4096], [3235872, 4096], [3239968,
```



Ahora sí, analizando el fichero resultante y buscando la cadena UAM obtenemos:

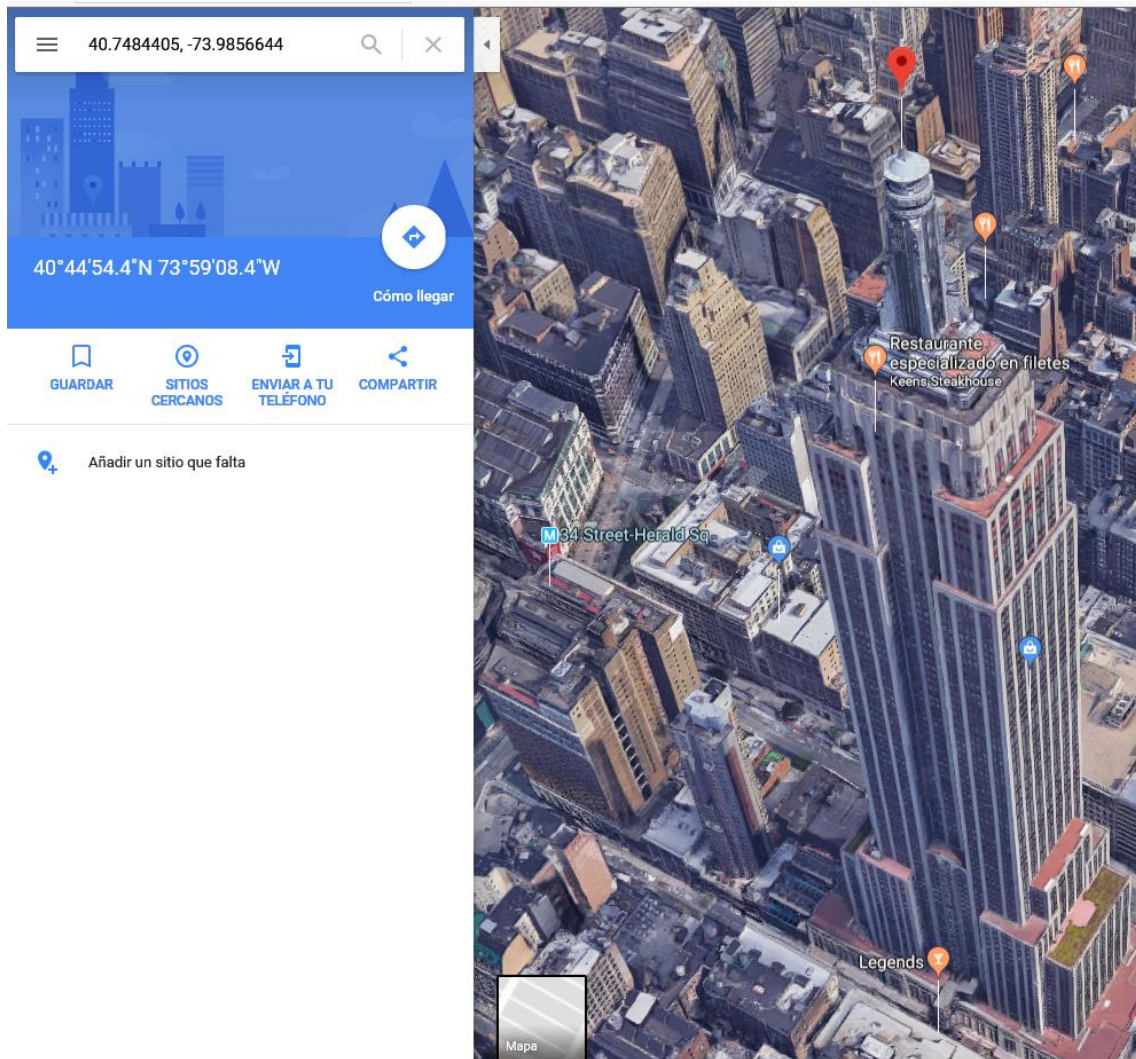
```
Users\anubis\AppData\Roaming\Microsoft\Windows\Recent\uam.lnk
Users\anubis\AppData\Roaming\Microsoft\Windows\Recent\uam (2).lnk
Users\anubis\AppData\Local\Temp\VirtualBox Dropped Files\2018-03-12T20_33_51.765201500Z\UAM(2)~1.JPG
$Recycle.Bin\S-1-5-~1\SRGKWFUM.jpg

$FILE_NAME
Creation                               Modified                               MFT Altered                               Access Date
Name/Path
-----
2018-03-12 20:33:51 UTC+0000 2018-03-12 20:33:51 UTC+0000 2018-03-12 20:33:51 UTC+0000 2018-03-12
20:33:51 UTC+0000 Users\anubis\Desktop\uam.jpg
$OBJECT_ID
Object ID: dec70d8f-3426-e811-9f5d-08002736a682
Birth Volume ID: 80000000-a000-0000-0000-180000000100
Birth Object ID: 81000000-1800-0000-3c68-746d6c3e0d0a
Birth Domain ID: 093c6865-6164-3e0d-0a09-093c7469746c
$DATA
0000000000: 3c 68 74 6d 6c 3e 0d 0a 09 3c 68 65 61 64 3e 0d <html>...<head>.
0000000010: 0a 09 09 3c 74 69 74 6c 65 3e 43 6f 6f 72 64 65 ...<title>Coorde
0000000020: 6e 61 64 61 73 20 64 65 20 4d 6f 72 66 65 6f 3c nadas.de.Morfeo<
0000000030: 2f 74 69 74 6c 65 3e 0d 0a 09 3c 2f 68 65 61 64 /title>...</head>
0000000040: 3e 0d 0a 09 3c 62 6f 64 79 3e 0d 0a 09 09 3c 68 >...<body>...<h
0000000050: 31 3e 34 30 2e 37 34 38 34 34 30 35 2c 20 2d 37 1>40.7484405,-7
0000000060: 33 2e 39 38 35 36 36 34 34 3c 2f 68 31 3e 0d 0a 3.9856644</h1>..
0000000070: 09 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c .</body>...</html>

$FILE_NAME
Creation                               Modified                               MFT Altered                               Access Date
Name/Path
-----
2018-03-11 14:38:29 UTC+0000 2018-03-11 14:38:29 UTC+0000 2018-03-12 17:50:40 UTC+0000 2018-03-11
14:38:29 UTC+0000 $Recycle.Bin\S-1-5-~1\SRGKWFUM.jpg
$OBJECT_ID
Object ID: 6f07a6c8-1d26-e811-bfd2-08002736a682
Birth Volume ID: 80000000-8800-0000-0000-180000000100
Birth Object ID: 6e000000-1800-0000-3c68-746d6c3e0d0a
Birth Domain ID: 093c6865-6164-3e0d-0a09-093c7469746c
$DATA
0000000000: 3c 68 74 6d 6c 3e 0d 0a 09 3c 68 65 61 64 3e 0d <html>...<head>.
0000000010: 0a 09 09 3c 74 69 74 6c 65 3e 55 41 4d 20 46 4c ...<title>UAM.FL
0000000020: 41 47 3c 2f 74 69 74 6c 65 3e 0d 0a 09 3c 2f 68 AG</title>...</h
0000000030: 65 61 64 3e 0d 0a 09 3c 62 6f 64 79 3e 0d 0a 09 ead>...<body>...
0000000040: 09 3c 68 31 3e 55 41 4d 7b 4e 33 30 5f 69 35 5f .<h1>UAM{N30_i5_
0000000050: 34 5f 47 30 44 7d 3c 2f 68 31 3e 0d 0a 09 3c 2f 4_G0D}</h1>...</
0000000060: 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e body>...</html>
```

En el fichero ‘\$RGKWFUM.jpg’ de la papelera de reciclaje vemos que contiene una flag del tipo **UAM{N30\_i5\_4\_G0D}** pero puesto que buscamos una localización revisamos los datos del otro fichero ‘uam.jpg’ que como título tiene “Coordenadas de Morfeo” y nos da las coordenadas **40.7484405, -73.9856644**.

Asumiendo que esas coordenadas son longitud y latitud, las ponemos en un servicio de coordenadas (por ejemplo, Google Maps) y nos mostrará su ubicación física:



Así que Morfeo está en el Empire State Building, y la flag será:

**UAM{Empire\_State\_Building}**

## REFERENCIAS

<http://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/>  
<https://w00tsec.blogspot.com.es/2015/02/extracting-raw-pictures-from-memory.html>  
<https://github.com/fireeye/Volatility-Plugins/tree/master/shimcachemem>  
<https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage>  
<https://backtrackacademy.com/articulo/forensic-analysis-extracting-and-reconstructing-images-from-memory-dumps>  
<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Gui>  
<https://volatility-labs.blogspot.com.es/2012/09/movp-34-recovering-tagclipdata-whats-in.html>  
[https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet\\_v2.4.pdf](https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf)  
<http://www.pentestingexperts.com/windows-gui-memory-forensics-clipboard-windows-atoms-message-and-event-hooks/>  
<http://www.pentestingexperts.com/windows-gui-forensics-session-objects-window-stations-and-desktop/>  
<https://cquireacademy.com/blog/forensics/memory-dump-analysis>  
<https://steemit.com/security/@nybble/forensic-extracting-files-from-mft-table-with-volatility-part-2-en>  
<https://www.evild3ad.com/956/volatility-memory-forensics-basic-usage-for-malware-analysis/>