```
Autor: Luis Fueris Martín
Fecha: 26-09-2016
Coms: Documentación sobre las herramientas utilizadas en
      la imagen [cfreds_2015_data_leakage_pc.dd].
URL: http://www.cfreds.nist.gov/data_leakage_case/data-leakage-case.html
```

Documentación

kpartx - esta herramienta lee de la tabla de particiones del backup y crea un mapeo en el dispositivo [/dev/loop[0-7]] en el cual están las particiones creadas. Esto es llamado creación (o eliminación) en caliente.

Ejemplo man

```
--------------------------------------------------------------------
To mount all the partitions in a raw disk image:

              kpartx -av disk.img

This will output lines such as:

              loop3p1 : 0 20964762 /dev/loop3 63

The loop3p1 is the name of a device file under /dev/mapper which you
can use to access the partition, for example to fsck it:

              fsck /dev/mapper/loop3p1

When you're done, you need to remove the devices:

              kpartx -d disk.img
--------------------------------------------------------------------
```

Montamos los dispositivos [/dev/mapper/loop0p[12]]:

```
$> sudo mount -o ro,noexec,nodev,nosuid /dev/mapper/loop0p1 /mnt/windows/pc1/
$> sudo mount -o ro,noexec,nodev,nosuid /dev/mapper/loop0p2 /mnt/windows/pc2/
```

Herramienta de [Linux] para manipular los registros de [Windoze]:

```
>> Forensic Registry EDitor
$> wget -q http://deb.pinguin.lu/debsign_public.key -O- | sudo apt-key add -
```

Nos descargamos el [*.deb], en [https://pinguin.lu/pkgserver]

Sin embargo da muchos problemas en cuanto a su instalación... Es mejor utilizar el comando [chntpw]. Con la opción [-e]

```
-----------------------------------------------------------------------
-e     Registry editor with limited capabilities (but it  does  include
       write support). For a slightly more powerful editor see reged
-----------------------------------------------------------------------
```

Nueva herramienta para visualizar los registros de [Windoze] en [Linux]
-> [RegRipper]

Instalación:

```
--------------------------------------------------------------------
```

DEBIAN/UBUNTU

```
$> apt-get install cpanminus make unzip wget
```

FEDORA

```
$> dnf install perl-App-cpanminus.noarch make unzip wget perl-Archive-\
Extract-gz-gzip.noarch which
```

CENTOS/REDHAT

```
$> yum install  perl-App-cpanminus.noarch make unzip wget perl-Archive-\
Extract-gz-gzip.noarch which

$> mkdir /usr/local/lib/rip-lib
$> wget https://github.com/keydet89/RegRipper2.8
$> cpanm -l /usr/local/lib/rip-lib Parse::Win32Registry

$> perl -pi -e 's/\r\n/\n/g' rip.pl
$> chmod +x rip.pl
```

Exit the first line of rip.pl to use your systems perl interpreter to \
run rip.pl

```
$> which perl | sed 's/\//\\\//g' > /tmp/perlloc && sed -i \
"s/ c:\\\\perl\\\\bin\\\\perl.exe/`cat /tmp/perlloc`/" rip.pl
```

Add/Modify a few commands to allow the RegRipper plugins directory to be found:

```
$> echo $PWD | sed 's/\//\\\//g' > /tmp/pwd && sed -i \
"s/use Getopt::Long;/use Getopt::Long;\nuse lib \'`cat /tmp/pwd`\/\';\n/" rip.pl

$> sed -i "s/plugindir = \"plugins\\\\\\\\/plugindir = \
\"`cat /tmp/pwd`\/plugins\//" rip.pl

$> sed -i 's/require "plugins\\\\".$plugins{$i}."\\.pl";/require \
"plugins\/".$plugins{$i}."\\.pl";/' rip.pl

--------------------------------------------------------------------
```

[cpanm] es una herramienta para conseguir, descomprimir, construir e instalar modulos de Perl.

Ejemplo [RegRipper]

```
-------------------------------------------------------------------------------
[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Windows/\
System32/config/SAM -f sam

Parsed Plugins file.
Launching samparse v.20160203
samparse v.20160203
(SAM) Parse SAM file for user & group mbrshp info


User Information
-------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
Login Count     : 6
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password not required
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : informant [1000]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 14:33:54 2015 Z
Name            :
Password Hint   : IAMAN
Last Login Date : Wed Mar 25 14:45:59 2015 Z
Pwd Reset Date  : Sun Mar 22 14:33:54 2015 Z
Pwd Fail Date   : Wed Mar 25 14:45:43 2015 Z
Login Count     : 10
  --> Password not required
  --> Password does not expire
  --> Normal user account

Username        : admin11 [1001]
Full Name       : admin11
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:51:54 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date  : Sun Mar 22 15:52:10 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 2
  --> Password does not expire
  --> Normal user account

Username        : ITechTeam [1002]
Full Name       : ITechTeam
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:52:30 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Sun Mar 22 15:52:45 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : temporary [1003]
Full Name       : temporary
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Sun Mar 22 15:53:01 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:55:57 2015 Z
Pwd Reset Date  : Sun Mar 22 15:53:11 2015 Z
Pwd Fail Date   : Sun Mar 22 15:56:37 2015 Z
Login Count     : 1
  --> Password does not expire
  --> Normal user account

-------------------------
Group Membership Information
-------------------------
Group Name    : Power Users [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Power Users are included for backwards compatibility and
possess limited administrative powers
Users         : None

Group Name    : Remote Desktop Users [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members in this group are granted the right to logon remotely
Users         : None

Group Name    : Backup Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Backup Operators can override security restrictions for
the sole purpose of backing up or restoring files
Users         : None

Group Name    : Guests [1]
LastWrite     : Wed Mar 25 10:15:19 2015 Z
Group Comment : Guests have the same access as members of the Users
group by default, except for the Guest account which is further restricted
Users :
  S-1-5-21-2425377081-3129163575-2985601102-501

Group Name    : Administrators [4]
LastWrite     : Sun Mar 22 15:52:30 2015 Z
Group Comment : Administrators have complete and unrestricted access
to the computer/domain
Users :
  S-1-5-21-2425377081-3129163575-2985601102-1000
  S-1-5-21-2425377081-3129163575-2985601102-500
  S-1-5-21-2425377081-3129163575-2985601102-1001
  S-1-5-21-2425377081-3129163575-2985601102-1002

Group Name    : Replicator [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Supports file replication in a domain
Users         : None

Group Name    : Cryptographic Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members are authorized to perform cryptographic operations.
```

```
Users         : None

Group Name    : Users [5]
LastWrite     : Sun Mar 22 15:53:01 2015 Z
Group Comment : Users are prevented from making accidental or
intentional system-wide changes and can run most applications
Users :
  S-1-5-21-2425377081-3129163575-2985601102-1002
  S-1-5-21-2425377081-3129163575-2985601102-1001
  S-1-5-21-2425377081-3129163575-2985601102-1003
  S-1-5-11
  S-1-5-4

Group Name    : Performance Monitor Users [0]
LastWrite     : Tue Jul 14 04:45:46 2009 Z
Group Comment : Members of this group can access performance counter data
locally and remotely
Users         : None

Group Name    : Distributed COM Users [0]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Members are allowed to launch, activate and use Distributed
COM objects on this machine.
Users         : None

Group Name    : Event Log Readers [0]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Members of this group can read event logs from local machine
Users         : None

Group Name    : Performance Log Users [0]
LastWrite     : Tue Jul 14 04:45:46 2009 Z
Group Comment : Members of this group may schedule logging of performance
counters, enable trace providers, and collect event traces both locally and
via remote access to this computer
Users         : None

Group Name    : IIS_IUSRS [1]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Built-in group used by Internet Information Services.
Users :
  S-1-5-17

Group Name    : Network Configuration Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members in this group can have some administrative privileges
to manage configuration of networking features
Users         : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
     - S-1-5-4  = Interactive
     - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin

samparse complete.
-------------------------------------------------------------------------------
```

Para extraer de los registros el [Hash] de los passwords.

Normally, Windows store passwords on single computer systems in the registry in a hashed format using the NTLM algorithm. The registry file is located in

C:\windows\system32\config\SAM.

This area of the registry has restrictive permissions so that a normal user cannot see the contents of HKLM\SAM deep enough to access the hash. In order to view the hashes one must change the permissions on the registry keys, this requires an administrative account on the system in Windows XP. I am unsure if access is possible using an administrator account in Vista or 7.

Once one has access to the password hashes though, it is difficult to gain the passwords again. There are many places on the internet that you can find information about brute forcing a NTLM hash. However, if you are simply trying to reset a password, I would recommend using Offline NT Password and Registry Editor.

If you want to get your arms wet though, the hash is stored under the key

HKLM\SAM\SAM\Domains\Account\Users\00000XXX

with a value named V. The hash is stored at a variable offset that is stored at offset 0x9C and is a 4 byte little endian value.

Otra herramientas interesante para realizar un dump de los [hashes]:

Physical access

df -Given physical access to the system, typically during a laptop assessment or a successful social engineering engagement, the preferred way to safely dump the password hashes is to power off the machine, enter the BIOS menu at power-on time, review the boot order to allow boot from the optical drive and USB drive before local hard-disk, save the settings and reboot the system with your favourite GNU/Linux live distribution CD or USB stick. Two widely known tools to dump the local users' hashes from the SAM file, given the Windows file system block file, are bkhive and samdump2:

```
    bkhive - dumps the syskey bootkey from a Windows system hive.
    samdump2 - dumps Windows 2k/NT/XP/Vista password hashes.
```

These tools are generally included in many GNU/Linux live distributions.
If they're not, make sure to bring a copy of them with you.
Usage:

```
    # bkhive
    bkhive 1.1.1 by Objectif Securite
    http://www.objectif-securite.ch
    original author: ncuomo@studenti.unina.it

    Usage:
    bkhive systemhive keyfile

    # samdump2
    samdump2 1.1.1 by Objectif Securite
    http://www.objectif-securite.ch
    original author: ncuomo@studenti.unina.it

    Usage:
    samdump2 samhive keyfile
```

Example of retrieving the SAM hashes from a Windows partition /dev/sda1:

```
    # mkdir -p /mnt/sda1
    # mount /dev/sda1 /mnt/sda1
    # bkhive /mnt/sda1/Windows/System32/config/SYSTEM /tmp/saved-syskey.txt
    # samdump2 /mnt/sda1/Windows/System32/config/SAM /tmp/saved-syskey.txt > /tmp/hashes.txt
```

[bkhive] se descarga pero no se instala... la solución es la siguiente:

The apt-get install bkhive command runs, but bkhive is not actually installed. I

found this workaround, however, downgrading to previous versions of bkhive and pwdump2:

```
$> apt-get purge bkhive
$> apt-get purge pwdump2
$> apt-get purge samdump2
$> curl http://http.us.debian.org/debian/poo...1-1.1_i386.deb > samdump2_1.1.1-1.1_i386.deb
$> dpkg -i samdump2_1.1.1-1.1_i386.deb
$> curl http://http.us.debian.org/debian/poo...1.1-1_i386.deb > bkhive_1.1.1-1_i386.deb
$> dpkg -i bkhive_1.1.1-1_i386.deb
```

https://packages.debian.org/source/wheezy/bkhive

After that bkhive and pwdump2 work.

Para abrir archivos [.ost y .pst] utilizaremos la herramienta [lspst]. (No funciona
con [.ost])

Una herramienta insteresante para recuperar ficheros borrados es [scalpel].

```
$> sudo apt install scalpel
$> sudo scalpel /dev/mapper/loop0p2 -o ~/Escritorio/scalpel/
```

El directorio destino debe estar vacío. Mucha información recabada con esta herramienta.

También está [Foremost]

Foremost : Forensics utility is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery. You can install it in Ubuntu and its derivatives by typing

----

```
$> sudo apt install foremost
$> sudo foremost -t pdf -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost
$> sudo foremost -t all -i /dev/mapper/loop0p2 -o ~/Escritorio/Foremost
```

Para extraer los [ShellBags], es decir, las trazas de que directorios ha estado entrando y saliendo un determinado usuario, se puede utilizar [sbag] (EN PRUEBA, PROBLEMAS CON LICENCIA??)

Otra herramienta interesante para extraer las ultimas ejecuciones de diversos programas sería [ShimCacheParser]. Es utilizada para extraer la cache llamada [Application Compatibility Cache] ("Shimcache").

- https://github.com/leviathan2701/ShimCacheParser

```
$> git clone https://github.com/leviathan2701/ShimCacheParser
```

Un ejemplo de su ejecución sería:

```
$> sudo python ShimCacheParser.py -v -i /mnt/windows/hdd/Windows/System32/config/SYSTEM -t -o SYSTEMCfreds.txt
```

```
$> git clone https://github.com/leviathan2701/ShimCacheParser
```

Un ejemplo de su ejecución sería:

```
$> sudo python ShimCacheParser.py -v -i /mnt/windows/hdd/Windows/System32/config/SYSTEM -t -o SYSTEMCfreds.txt
```

During a recent investigation, we found references to timestamps associated with probable malicious files that preceded the earliest known date of compromise. These Application Compatibility Cache (“Shimcache”) timestamps were the only evidence linked to this timeframe.

The Windows Shimcache was created by Microsoft beginning in Windows XP to track compatibility issues with executed programs. The cache stores various file metadata depending on the operating system, such as:

File Full Path
File Size
$Standard_Information (SI) Last Modified time
Shimcache Last Updated time
Process Execution Flag

Similar to a log file, the Shimcache also "rolls" data, meaning that the oldest data is replaced by new entries. The amount of data retained varies by operating system.
Additional information on Shimcache can be found in the Mandiant blog post by Andrew Davis.

It is important to understand there may be entries in the Shimcache that were not actually executed. Based on our current understanding of the Shimcache, there are two actions that can cause the Shimcache to record an entry:

    A file is executed. This is recorded on all versions of Windows beginning with XP.
    On Windows Vista, 7, Server 2008, and Server 2012, the Application Experience
        Lookup Service may record Shimcache entries for files in a directory that a user
        interactively browses. For example, if a directory contains the files “foo.txt”
        and “bar.exe”, a Windows 7 system may record entries for these two files in the Shimcache.

Microsoft designed the Shimcache in Windows Vista, 7, Server 2008 and Server 2012 to incorporate a "Process Execution Flag" category for each entry. The actual name and true purpose of this flag is still unknown, however, we have observed that the Client/Server Runtime Subsystem (CSRSS) process will set this flag during process creation/execution on those operating systems. Simply put, the Process Execution Flag, where present, makes it easier for the investigator to determine whether or not an entry was executed or if this entry was added a result of an activity other than file execution, such as interactively browsing a directory. These entries can be easily spotted by observing if the Process Execution Flag is marked as FALSE. Below is an example of entries from a Windows Server 2012 Shimcache. Notice the two entries which were not executed.

URL [http://forensicsblog.org/tag/mounting-shadow-copies/]
URL [http://epyxforensics.com/]
URL [https://msdn.microsoft.com/en-us/library/windows/desktop/aa384612(v=vs.85).aspx]
Más herramientas utilizadas [sleuthkit]:

```
$>  sudo apt-get install sleuthkit
```

Además de [libvshadow]:

----

libvshadow by Joachim Metz is an excellent tool for conducting a deeper analysis of shadow copies. We’ll set up the tool’s requirements and set it up from its latest source below.

Instalamos las dependencias:

```
$> sudo apt install libfuse-dev --> NECESARIO?¿
$> sudo apt install libvshadow-utils
```

Para saber el offset:

```
[leviathan3773@latitude:System Volume Information ] $ mmls ~/Escritorio/cfreds/R
esources/DDs/cfreds_2015_data_leakage_pc.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000206847   0000204800   NTFS / exFAT (0x07)
003:  000:001   0000206848   0041940991   0041734144   NTFS / exFAT (0x07)
004:  -------   0041940992   0041943039   0000002048   Unallocated
[leviathan3773@latitude:System Volume Information ] $
```

Ahora hay que multiplicar el punto de inicio, en este caso [206848] por 512 (105906176)

```
[sudo mount -t ntfs -o ro,offset=65536 shadows.dd /mnt/evidence]
```

Utlización:

```
$> vshadowinfo -o [offset] [image]
```

Ejemplo:

URL [http://epyxforensics.com/mounting-shadow-volumes-in-linux-ubuntu-12-04/]

```
[leviathan3773@latitude:~ ] $ sudo vshadowinfo -o 105906176 Escritorio/cfreds/Re
sources/DDs/cfreds_2015_data_leakage_pc.dd
vshadowinfo 20160110

Volume Shadow Snapshot information:
  Number of stores: 1

Store: 1
  Identifier    : 9b365826-d2ef-11e4-b734-000c29ff2429
  Shadow copy set ID  : 56e43eb5-ac18-4f06-a521-1e17712b7ced
  Creation time   : Mar 25, 2015 14:57:27.293805500 UTC
  Shadow copy ID    : 8f1a2a2d-ce6b-42a5-b92b-f13e65d9c2cb
  Volume size   : 21367881728 bytes
  Attribute flags   : 0x0042000d
```

Para montarlo correctamente:

```
[leviathan3773@latitude:~ ] $ sudo vshadowmount -o 105906176 Escritorio/cfreds/R
esources/DDs/cfreds_2015_data_leakage_pc.dd /mnt/vssvolume/
vshadowmount 20160110
```

Como podemos observar:

```
[leviathan3773@latitude:~ ] $ sudo ls -la /mnt/vssvolume
total 4
dr-xr-xr-x 2 root root           0 sep 22 12:27 .
drwxr-xr-x 4 root root        4096 sep 22 12:24 ..
-r--r--r-- 1 root root 21367881728 ene  1  1970 vss1
[leviathan3773@latitude:~ ] $
```

Puede haber algunos problemas:

```
[leviathan3773@latitude:mnt ] $ ls -lat
ls: no se puede acceder a 'vssvolume': Permiso denegado
total 12
drwxr-xr-x  4 root root 4096 sep 22 12:24 .
drwxr-xr-x 24 root root 4096 sep 21 09:43 ..
drwxr-xr-x  6 root root 4096 sep 12 14:45 windows
d?????????  ? ?    ?       ?            ? vssvolume
[leviathan3773@latitude:mnt ] $ ls -lat vssvolume
ls: no se puede acceder a 'vssvolume': Permiso denegado
[leviathan3773@latitude:mnt ] $ sudo ls -lat vssvolume
total 4
dr-xr-xr-x 2 root root           0 sep 22 12:27 .
drwxr-xr-x 4 root root        4096 sep 22 12:24 ..
-r--r--r-- 1 root root 21367881728 ene  1  1970 vss1
[leviathan3773@latitude:mnt ] $
```

Solución

From here you can image, carve and/or use the sleuthkit against the vss1 shadow volume. To access the directory structure of the shadow volume we need to mount it using the mount command. But before we do that, we need to designate a location where we can temporarily mount the shadow volume as a file system. To keep things simple, let’s create a directory called vss1logical in the root of the mnt folder. Type the below command into the terminal and press enter. Type your root password (if needed).

```
sudo mkdir /mnt/vss1logical
```

To mount that shadow volume as a file system, type the following into the terminal.

```
sudo mount -o ro /mnt/vssvolume/vss1 /mnt/vss1logical/
```

Mount is the command to mount a file system. The -o flag specifies the options for mounting. In this instance we opted to mount it as a “ro” read-only file system. /Mnt/vssvolume/vss1 is the shadow volume, and /mnt/vss1logical/ is the mount point. Press enter, and type your root password (if needed).

Your shadow volume is now mounted as a file system under /mnt/vss1logical/. Change directory (cd) into the vss1logical directory and run ls -l.

```
[leviathan3773@latitude:mnt ] $ sudo mount -o ro,noexec,nosuid,nodev /mnt/vssvol
ume/vss1 /mnt/vss1logical/
[leviathan3773@latitude:mnt ] $ cd /mnt/vss1logical/
[leviathan3773@latitude:vss1logical ] $ ls
Documents and Settings  MSOCache      PerfLogs     Program Files        Recovery
      System Volume Information  Windows
hiberfil.sys            pagefile.sys  ProgramData  Program Files (x86)  $Recycle
.Bin  Users
[leviathan3773@latitude:vss1logical ] $ df -hT
S.ficheros                     Tipo     Tamaño Usados  Disp Uso% Montado en
udev                           devtmpfs   3,9G      0  3,9G   0% /dev
tmpfs                          tmpfs      788M   9,5M  779M   2% /run
/dev/sdb1                      ext4       103G    81G   17G  83% /
```

```
tmpfs                         tmpfs      3,9G   560K  3,9G   1% /dev/shm
tmpfs                         tmpfs      5,0M   4,0K  5,0M   1% /run/lock
tmpfs                         tmpfs      3,9G      0  3,9G   0% /sys/fs/cgroup
tmpfs                         tmpfs      788M    96K  788M   1% /run/user/1000
/home/leviathan3773/.Private ecryptfs   103G    81G   17G  83% /home/leviathan37
73
/dev/mapper/loop0p2           fuseblk     20G    17G  3,4G  84% /mnt/windows/hdd
/dev/mapper/loop1p1           vfat      1020M   224M  797M  22% /mnt/windows/rm2
/dev/loop2                    udf        703M   703M     0 100% /media/leviathan3
773/IAMAN CD
/dev/sda2                     fuseblk    112G   106G  6,3G  95% /media/leviathan3
773/E062E8AC62E8891C
/dev/loop4                    fuseblk     20G    18G  2,8G  87% /mnt/vss1logical
[leviathan3773@latitude:vss1logical ] $
```

Una herramienta para ver archivos que han sido eliminador de [SQLite] sería:

- [https://github.com/mdegrazia/SQLite-Deleted-Records-Parser]

Su uso sería el siguiente:

```
$> sudo python sqlparse_v1.3.py  -f /mnt/vss1logical/Users/informant/AppData/Loc
al/Google
   /Drive/user_default/snapshot.db -o report.tsv

Type        Offset  Length  Data
Unallocated 1034    986     v EK M 0Bz0ye6gXtiZaVl8yVU5mWHlGbWcdo_u_wanna_build_
a_snow_man.mp3TUxmho2c4553f99533d85adb104b3a5c38521afilej/ M 0Bz0ye6gXtiZaakx6d3
R3c0JmM1Uhappy_holiday.jpgTUxj0c77d6a2704155dbfdf29817769b7478file
Unallocated 3080  1016  #E0Bz0ye6gXtiZaVl8yVU5mWHlGbWcroot%0Bz0ye6gXtiZaakx6d3R3
c0JmM1Uroot
Unallocated 7186  206 rN##Utablecloud_entrycloud_entryCREATE TABLE cloud_entry (
doc_id TEXT, filename TEXT, modified INTEGER, created INTEGER, acl_role INTEGE
Unallocated 8202  964 *P^KMdo_u_wanna_build_a_snow_man.mp3A2#T(2c4553f99533d85ad
b104b3a5c38521ahoKY/Mhappy_holiday.jpgA2`0c77d6a2704155dbfdf29817769b7478
Unallocated 9232  324 ) ` tablemappingmappingCREATE TABLE mapping (inode_number
INTEGER, doc_id TEXT, UNIQUE (inode_number), FOREIGN KEY (inode_number) REFERENC
ES local_entry(inode_number), FOREIGN KEY (doc_id) REFERENCES cloud_entry(doc_id
))- Aindexsqlite_autoindex_mapping_1mapping,##tablelocal_
Unallocated 10248 1016  %)%)
Unallocated 13322 997 'E0Bz0ye6gXtiZaVl8yVU5mWHlGbWc)E0Bz0ye6gXtiZaakx6d3R3c0JmM
1U
Unallocated 19464 1016  }8w \\?\C:\Users\informant\Google Drive\happy_holiday.jp
gG \\?\C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3
```