QUANTIKA

Curso de Ciberseguridad

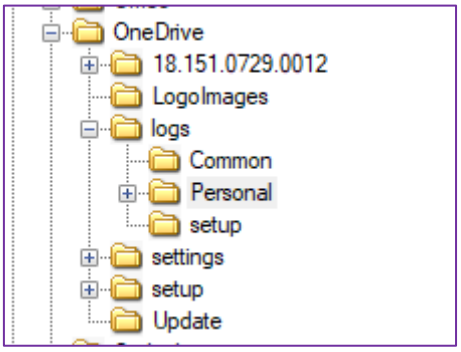
Análisis Forense en Windows

Análisis Forense Informático

ONEDRIVE

Onedrive es un servicio de alojamiento de ficheros en la nube que muchas veces, puede ser objeto de una investigación forense. Existe una aplicación de sincronización de ficheros, la cual se instala Windows y transfiere de manera automática todos los ficheros hacia el Cloud. La ruta de configuración del aplicativo se puede localizar en:

- **\Users\usuario\AppData\Local\Microsoft\OneDrive\logs**



Dentro de la carpeta Personal podemos encontrar:

- Ficheros SyncEngine relacionados con la sincronización con OneDrive
- Fichero SyncDiagnostic.log: contiene un informe de diagnóstico con multitud de campos que podemos analizar a continuación:

SYNCDIAGNOSTIC.LOG

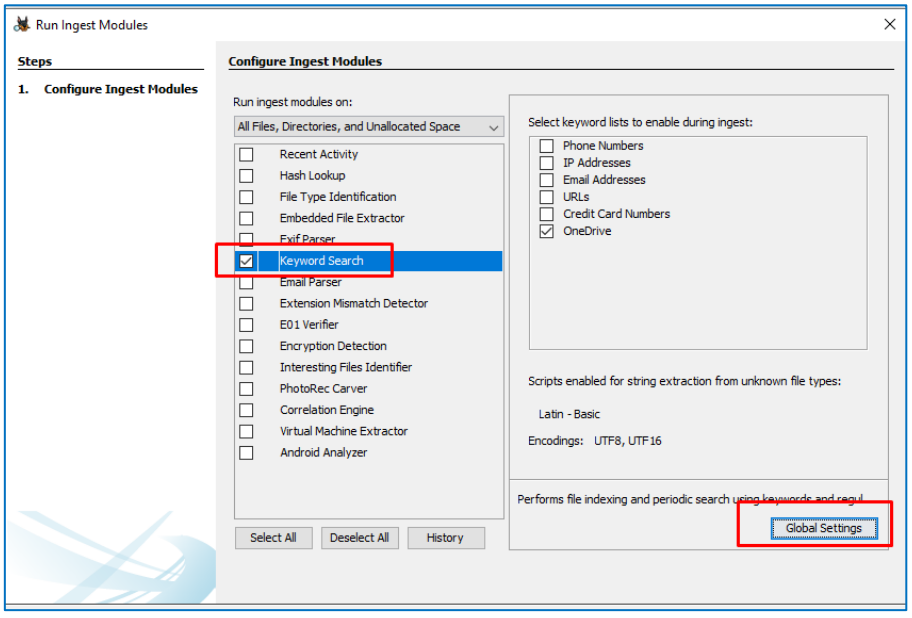
Información de los ficheros que sincronizados:

- Tamaño en bytes
- Fecha de creación en el sistema de Archivos en UTC en formato epoch
- Fecha de modificación en el sistema de Archivos en UTC en formato epoch
- Total, de ficheros en el cloud de Onedrive
- Total, de ficheros en la carpeta de OneDrive
- CID: es el identificador único del usuario en Onedrive
- Marcas de tiempo en UTC de cuando se genera el reporte
- Tamaño total del disco del sistema operativo.

```
Scanning '%MountPoint%[62014A3CFEC60D07!101]\NewSeaLab\CakeHerWag'

    - file   'C:\Users\ismis\OneDrive\Escritorio\Tools\know-your-file-
types.jpg', size=117888, creationTime=1538599456, modTime=1538599457, isOcsi=0

    - file   'C:\Users\ismis\OneDrive\Escritorio\Tools\slacker.exe',
size=53248, creationTime=1538599361, modTime=1538599346, isOcsi=0

    - file   'C:\Users\ismis\OneDrive\Escritorio\Tools\time.exe', size=57344,
creationTime=1538598412, modTime=1538598383, isOcsi=0

Folder '%MountPoint%[62014A3CFEC60D07!101]\NewSeaLab\CakeHerWag' Total: 0
folders (0 sub-scopes), 3 files


Cloud Total: 11 folders, 14 files (8967595 bytes)

Disk Total: 11 folders, 14 files (8967595 bytes)

DAT Total: 11 folders, 14 files (8967595 bytes)

cid = 62014a3cfec60d07

timeUtc = 2018-10-08T07:32:03.0000000Z
```

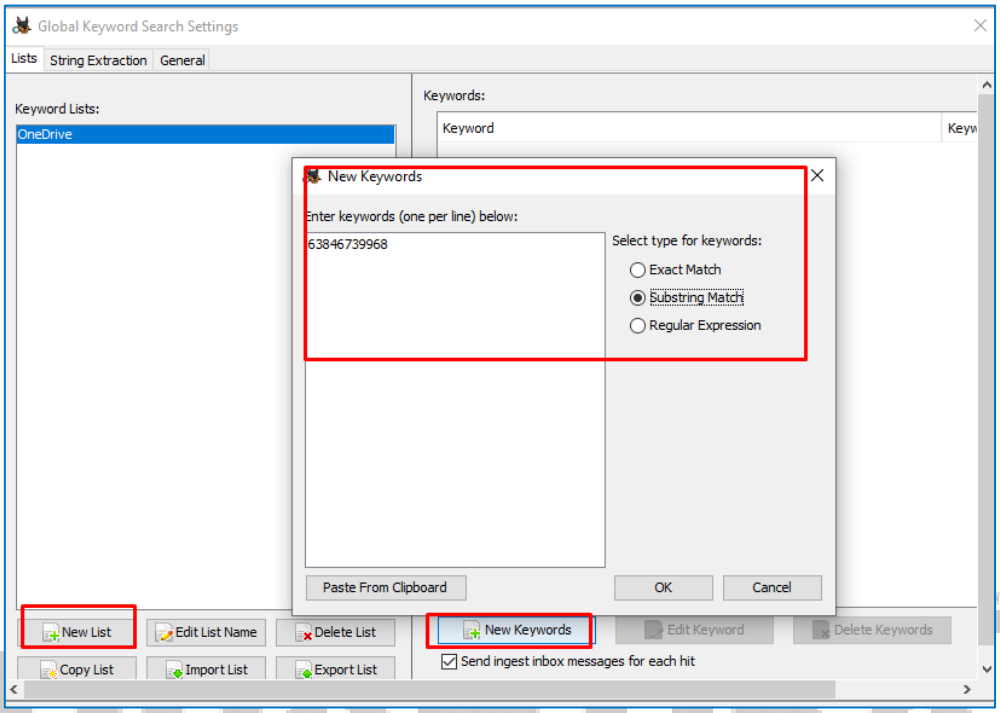
El CID es el campo que nos permitiría localizar todo lo relacionado con OneDrive en la evidencia que vayamos a analizar. Podríamos utilizar la herramienta Autopsy para realizar una búsqueda de este campo y ver que ficheros están involucrados.

Para ello previamente hay configurar Autopsy a la hora de crear el caso, de la siguiente manera:

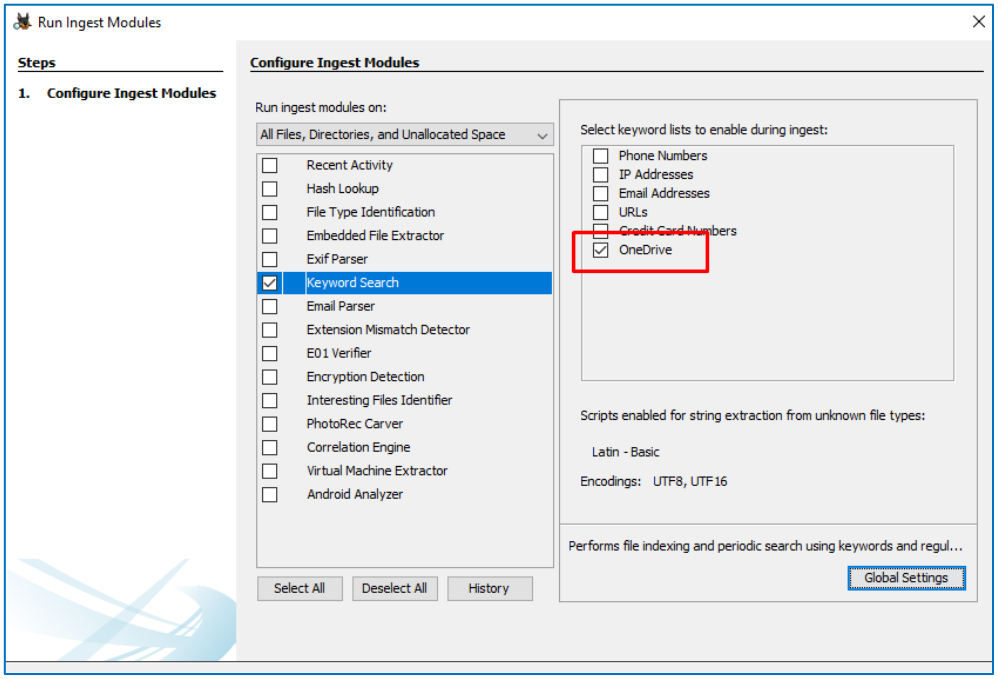


Nos podemos configurar una lista propia para buscar el String en cuestión mediante la opción de "Global Settings":

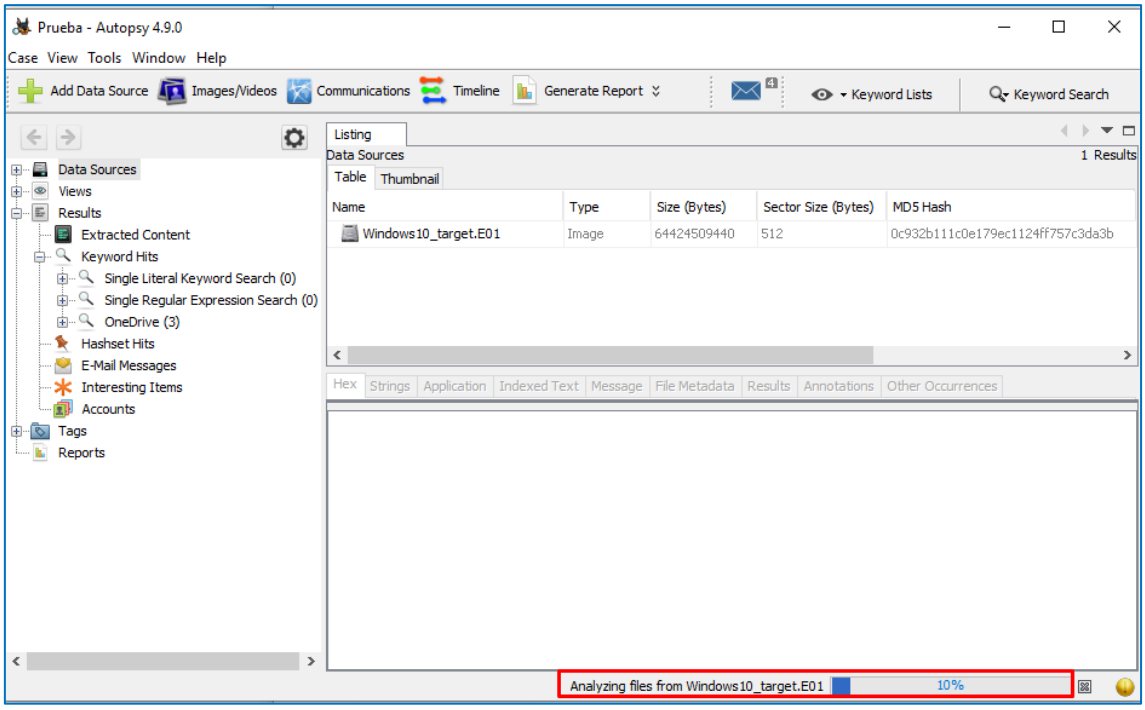
- New List: OneDrive
- New Keywords: metemos el CID como Substring



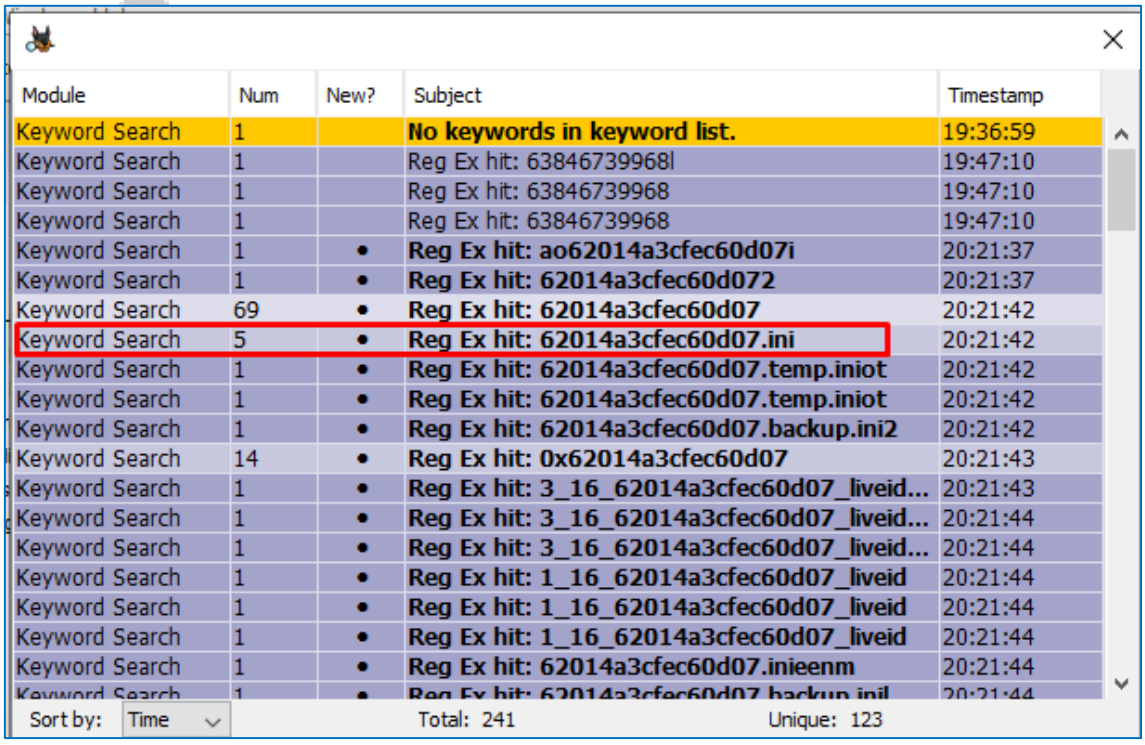
Marcamos nuestra nueva keyword:



Dejamos Autopsy trabajando:



A raíz de esta búsqueda podemos encontrar más ficheros involucrados en la configuración de OneDrive: **\Users\{usuario}\AppData\Local\Microsoft\OneDrive\settings\Personal\{CID}.ini**



Module	Num	New?	Subject	Timestamp
Keyword Search	1		**No keywords in keyword list.**	19:36:59
Keyword Search	1		Reg Ex hit: 63846739968l	19:47:10
Keyword Search	1		Reg Ex hit: 63846739968	19:47:10
Keyword Search	1		Reg Ex hit: 63846739968	19:47:10
Keyword Search	1	•	**Reg Ex hit: ao62014a3cfec60d07i**	20:21:37
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d072**	20:21:37
Keyword Search	69	•	**Reg Ex hit: 62014a3cfec60d07**	20:21:42
Keyword Search	5	•	**Reg Ex hit: 62014a3cfec60d07.ini**	20:21:42
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d07.temp.iniot**	20:21:42
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d07.temp.iniot**	20:21:42
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d07.backup.ini2**	20:21:42
Keyword Search	14	•	**Reg Ex hit: 0x62014a3cfec60d07**	20:21:43
Keyword Search	1	•	**Reg Ex hit: 3_16_62014a3cfec60d07_liveid...**	20:21:43
Keyword Search	1	•	**Reg Ex hit: 3_16_62014a3cfec60d07_liveid...**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 3_16_62014a3cfec60d07_liveid...**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 1_16_62014a3cfec60d07_liveid**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 1_16_62014a3cfec60d07_liveid**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 1_16_62014a3cfec60d07_liveid**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d07.inieenm**	20:21:44
Keyword Search	1	•	**Reg Ex hit: 62014a3cfec60d07.backup.inil**	20:21:44

Sort by: Time Total: 241 Unique: 123

Se localiza el fichero con extensión .ini

Keyword	62014a3cfec60d07.ini
Preview	«62014a3cfec60d07.ini«
File	/Users/ismis/AppData/Local/Microsoft/OneDrive/settings/Personal/62014a3cfec60d07.ini
List	OneDrive
Reg Ex	62014a3cfec60d07

{CID}.INI

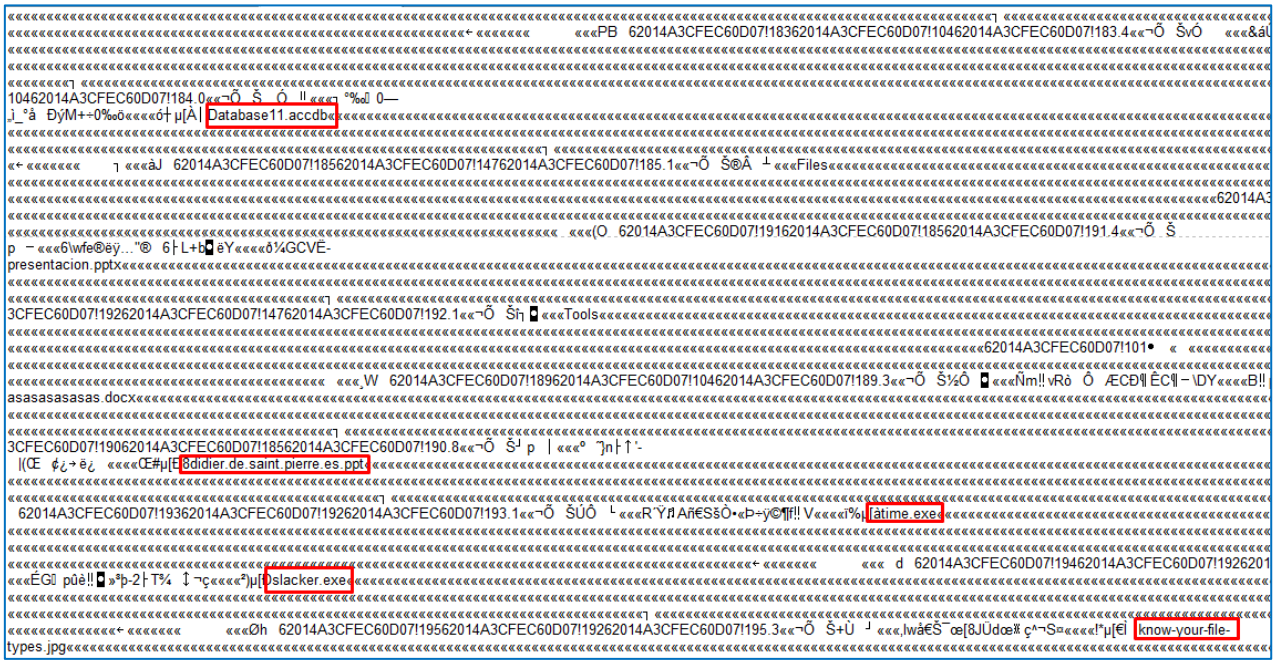
Contenido 62014a3cfec60d07.ini

```
library = 1 4 62014A3CFEC60D07!101 1538588103 "SkyDrive" Me personal "C:\Users\ismis\OneDrive" 104a5916f-a289-48e1-b3a4-8b3cce08c837
installID = 1
originatorID = 7ad443c0-d302-4a54-910b-57abde061c61
lastRefreshTime = 1538983918
requestsSent = 8
bytesTransferred = 73563
uploadLimitKbPerSec = 0
downloadLimitKbPerSec = 0
uploadSpeedAutoLimited = false
edpManaged = false
edpManagedSince = 0
needsPlaceholderTransition = false
OfficeOriginatorID = 2eaeb13d-453a-4a61-bf8b-8abd6ff765fe
Subscription = 8 62014A3CFEC60D07!101 push_WLS_SubscriptionId_dd85a3bf-58b2-4147-8f39-1f6bc678ebe7
Subscription = 2 62014A3CFEC60D07!101 WLS_SubscriptionId_1059BF66-7D02-4D73-9347-D6B4C228D6E1
Subscription = 1 62014A3CFEC60D07!101 WLS_SubscriptionId_A8705BA3-DF4F-439E-8812-A8A60275203B
```

- LastRefreshtime: formato epoc UTC
- BytesTransferred: bytes enviados al cloud
- Skydrive: ruta de lo que se debe sincronizar

{CID}.DAT

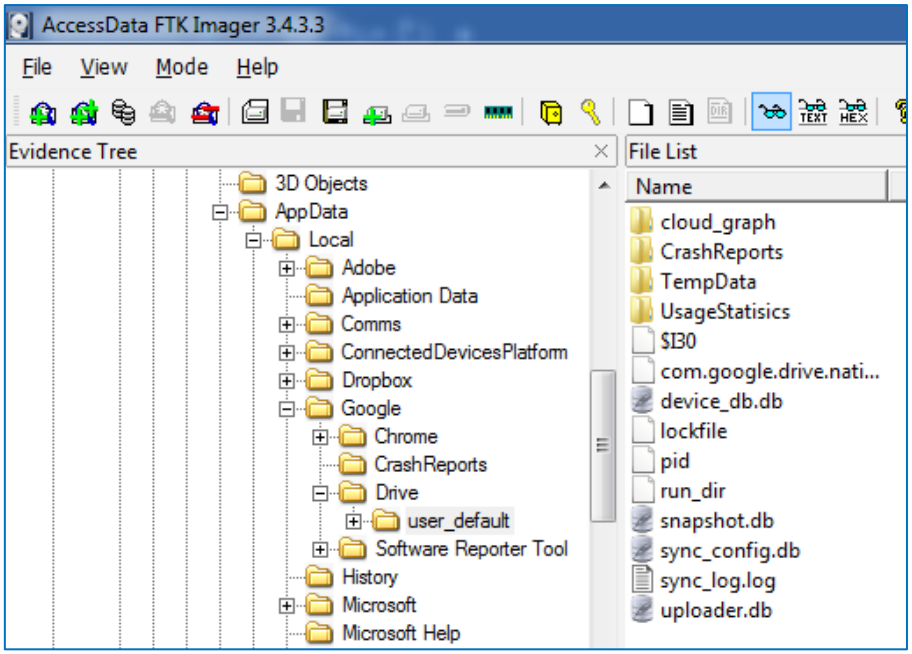
Dentro de la carpeta de personal, podemos el encontrar el fichero **62014a3cfec60d07.dat** que si lo abrimos con un editor hexadecimal como HxD podremos identificar los nombres de los ficheros y carpetas que se sincronizan con OneDrive.



GOOGLE DRIVE

Google Drive es otra herramienta que permite la sincronización de ficheros con la nube. Este tipo de herramientas puede ser siempre objeto de investigación en caso de una exfiltración de la misma. La ruta donde está la configuración de Google Drive es la siguiente:

- **\Users\{usuario}\AppData\Local\Google\Drive\user_default**



SYNC_LOG.LOG

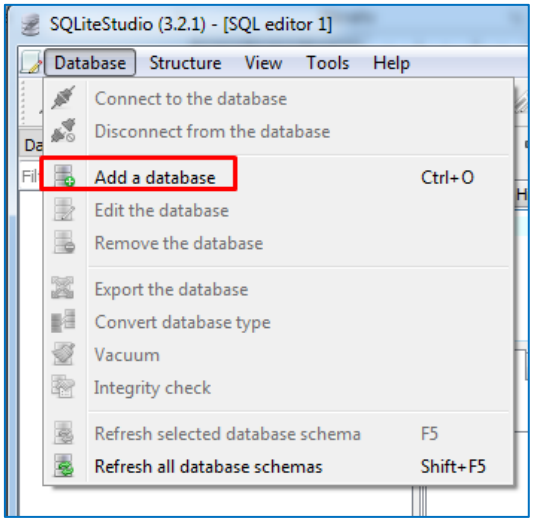
Contiene un log con toda la información del agente, rutas de sincronización con ficheros, ficheros a sincronizar, timestamps, MD5 de los ficheros, nombre de la cuenta asociada de Gmail.

```
Request (ismiserrani2345@gmail.com):
InsertFile(tags=Reason.CREATE_FILE(SyncType.UNKNOWN_SYNC_TYPE),
name=u'Word Document.docx',
media=DriveClientMediaFileUpload(BufferedStream(filename=u'\\\\?\C:\
\Users\\ismis\\OneDrive\\Documents\\Word Document.docx',
modified_date=1538592749, inode=LocalID(inode=1407374883640205L,
volume='serial:2317276588'), size=11465L, buffer_size=5242880),
mimetype='application/vnd.openxmlformats-officedocument.wordprocessin
gml.document', chunksize=-1, resumabe=False), modified=1538592749,
storage_mode=<StoragePolicyMode.ORIGINAL: 'original'>,
parent_id='1efrGWGKka9i9f353GKNV7y3qqtFvZNFr',
doc_id=u'1JoWUO-jAdUN4ouY_mRJrdznZGLYO0h8d')
Response:
File(size=11465L, md5_checksum=u'3dd9c5902d9614da3e32360ff4150145',
```

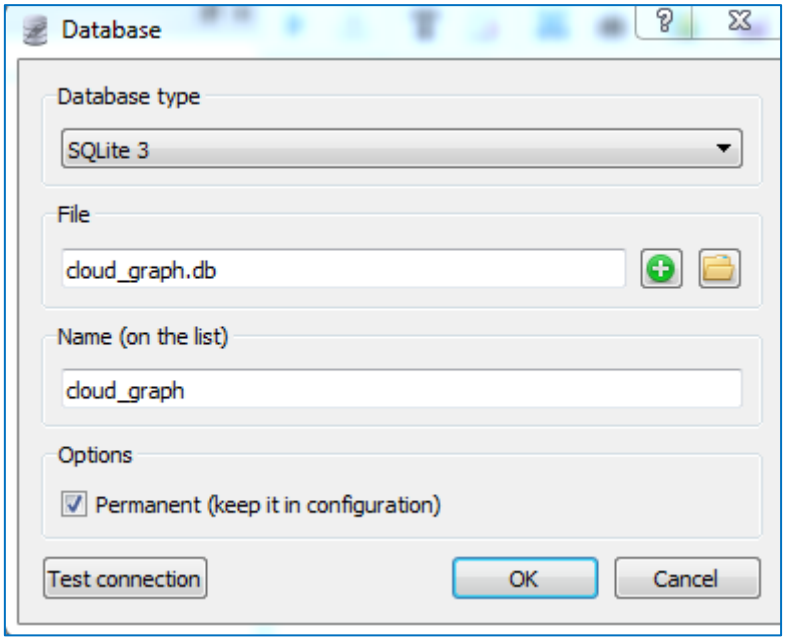
Si un fichero fuese borrado, aparecería también en este log, junto con su correspondiente MD5.

CLOUD_GRAPH\CLOUD_GRAPH.DB

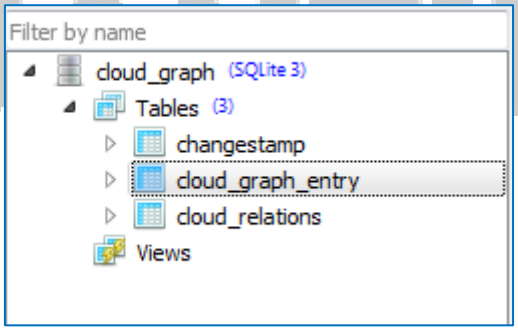
Es un fichero en SQLite y los podemos abrir con la herramienta SQLite Studio:



Y abrimos la base de datos que previamente hemos extraído como siempre.



La tabla más importante es: cloud_graph_entry



Podemos seleccionar la tabla, pinchar sobre la solapa DATA y ver los registros.

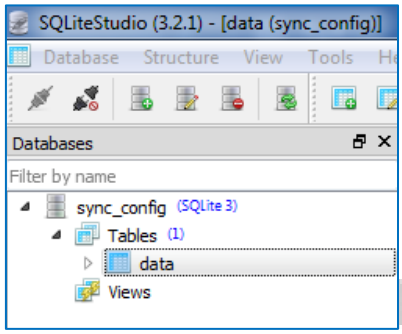
doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum
root	NULL	NULL	NULL	NULL	0	NULL	NULL	NULL
1wLR0YcZ88hJAvnIyedg-MIug_XBovNDt	My PC	1538590582	NULL	0	0	0	NULL	NULL
1efrGWGKka9i9f353GKNV7y3qqtFvZNFr	Documents	1538590584	NULL	0	0	0	NULL	NULL
1TaP2AWeXfs4baY1uTVBIUVC-70nQ-48j	Pictures	1538590589	NULL	0	0	0	NULL	NULL
1nwARTmuarwid4KrIcnqmq-VDT8aW5hIe	Saved Pictures	1538588219	NULL	0	0	0	NULL	NULL
1i6xlsM08W2evOEzABc1V6bWU56Mc2_E-	Capturas de pantalla	1538588219	NULL	0	0	0	NULL	NULL
1KkIpiaqdkqQR90t5vGZ7ByEOnTk0_as-	Álbum de cámara	1538588221	NULL	0	0	0	NULL	NULL
1LSIScBLGR3bGRxhg9aB8g56LMfZQ_Mrd	Custom Office Templates	1538592742	NULL	0	0	0	NULL	NULL
1JoWUO-jAdUN4ouY_mRJrdznZGLYO0h8d	Word Document.docx	1538592749	NULL	0	1	0	11465	3dd9c5902d9614da3e32360ff4150145
1VvcwUrahZVFV2OzAhnBkq5rFoBKKnZJc	Book1.xlsx	1538592925	NULL	0	1	0	8058	3b7940e6d54d2a8d3262ec1e15f3f88b
1cO5UEqS6Sxya7sI1-JweKkMmj6Ih_dKy	Database1.accdb	1538593007	NULL	0	1	0	561152	7bf912f200d12949695a6f4dfe5fe3d5
18VaJUcHhxp2iLfax-jIpYAGE3gYb4dvA	Database11.accdb	1538593011	NULL	0	1	0	376832	76852d782b79fe4b3cefa3b3dc1a8b1d
1gmbXjtYEvjRFU64-HpgaU_2H5rGkehgR	Book1.xlsx	1538592925	NULL	0	1	0	8058	3b7940e6d54d2a8d3262ec1e15f3f88b
1ILZTitLTD3CpWwiMNn-1bL65ryDK2Cw4	asasasasasas.docx	1538593602	NULL	0	1	0	11632	6065ae61d12479f1a1fbe0a01832037c

Podemos identificar:

- Nombres de los ficheros sincronizados
- Fecha de modificación en epoc UTC
- Tamaño
- Checksum que es el Hash MD5 del fichero.

SYNC_CONFIG.DB

Es otra base de datos SQLITE donde también puede encontrarse información muy significativa, como la cuenta de email asociada, ubicación de las carpetas compartidas, versión del Google Drive instalado. Solo contiene una tabla: data

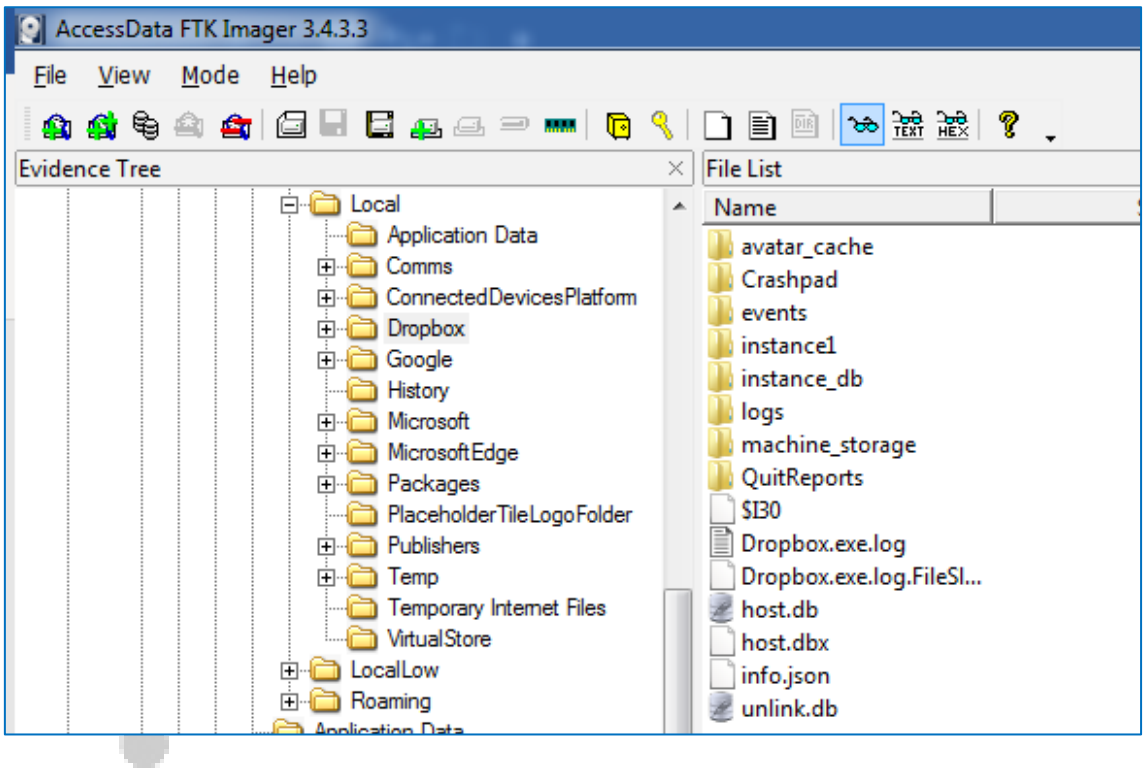


Configuración de la cuenta de Google Drive:

	entry_key	data_key	data_value
14	share_notification	value	1
15	local_sync_root_path	value	\\?\C:\Users\ismis\Google Drive
16	copy_duplicate_photos	value	1
17	user_email	value	ismiserrani2345@gmail.com
18	domain_policy	default_sync_all	1
19	domain_policy	domain_policy_description_url	
20	win10_icons_upgraded	value	1
21	autostart_upgraded	value	1
22	cloud_graph_generation	value	8
23	tango_storage	value	gAJ9cQFVC0NsaWVudFRva2VuVVRDaWNLSlF

DROPBOX

Para Dropbox, existe una versión del cliente en Windows el cual nos permite tener sincronizados todos nuestros ficheros y archivos en un directorio del equipo, de tal forma que podemos disponer de ellos de forma local en el equipo como cualquier otro fichero.



La forma que tiene de gestionar la aplicación de Windows para Dropbox, es mediante bases de datos SQLITE. En estas bases de datos, se almacena toda la información necesaria para el correcto funcionamiento y sincronización: los ficheros de configuración, cuenta de correo, así como todos los ficheros que el usuario tiene en su cuenta de Dropbox y cuales están y cuales no sincronizados en el equipo. Las bases de datos de Dropbox las podemos encontrar bajo la siguiente ruta:

- **\Users\%USERNAME%\AppData\Local\Dropbox**
- **\Users\%USERNAME%\AppData\Local\Dropbox\Instance1**
- **\Users\%USERNAME%\AppData\Roaming\Dropbox**

Las principales bases de datos que podemos encontrar bajo estos directorios son:

- Sigstore.dbx
- Filecache.dbx
- Deleted.dbx
- Config.dbx

Todas las bases de datos nombradas anteriormente tienen una extensión .dbx, esto quiere decir que son bases de datos cifradas. El cifrado utilizado por Dropbox es DPAPI: https://msdn.microsoft.com/en-us/library/ms995355.aspx

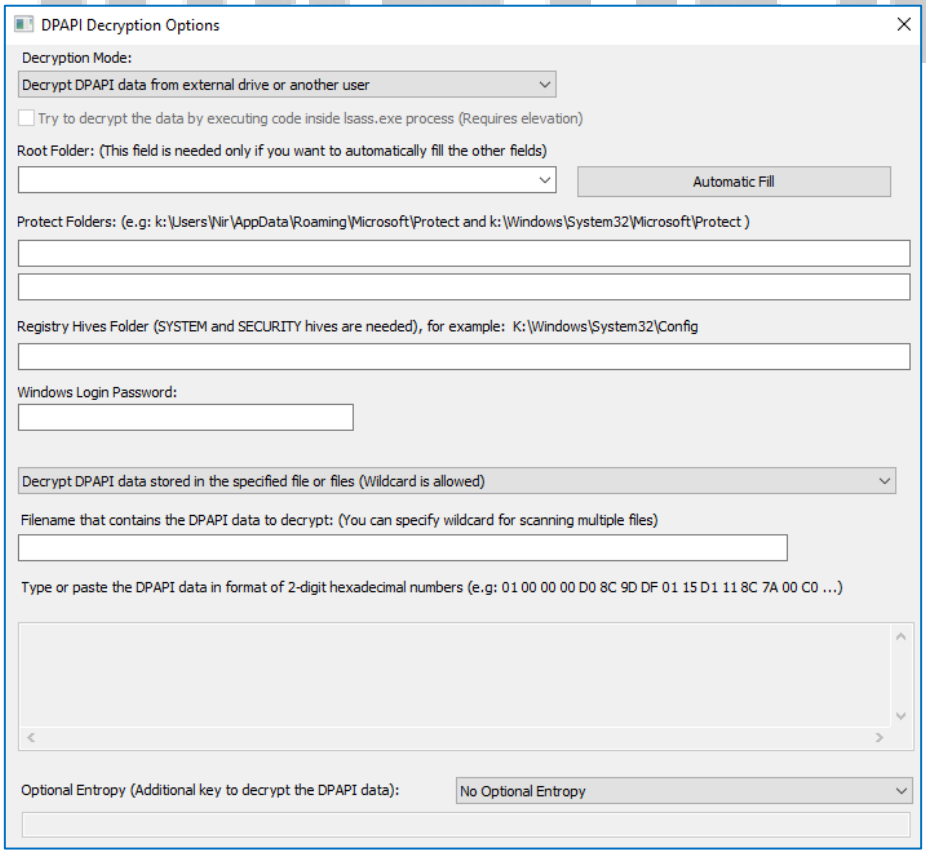
Para descifrar las bases de datos, utilizaremos la evidencia con la que hemos venido trabajado hasta ahora, el perfil Pedro, ya que el perfil de **Ismis** está asociado a cuenta de Outlook.

Para obtener más datos de cómo funciona el cifrado de Dropbox es necesario echar un vistazo a esta web http://blog.digital-forensics.it/2017/04/brush-up-on-dropbox-dbx-decryption.html y obtendremos:

- Entropía DPAPI para cifrar: D114A55212655F74BD772E37E64AEE9B
- La SALT que utiliza: 0D638C092E8B82FC452883F95F355B8E
- 1066 iteraciones usando PBKDF2

Dropbox utiliza una clave de cifrado para cifrar las bases de datos con extensión DBX. Esta clave de cifrado está cifrada en el registro de usuario, mediante DPAPI y con la entropía anteriormente identificada. Una vez que se descifra mediante DPAPI hay utilizar una función PBKDF de 1066 iteraciones con la salt indicada, para poder obtener la clave final del fichero DBX.

La herramienta que permite realizar descifrados externos de DPAPI con interfaz gráfica se llamada **DataProtectionDecryptor de Nirsoft:**

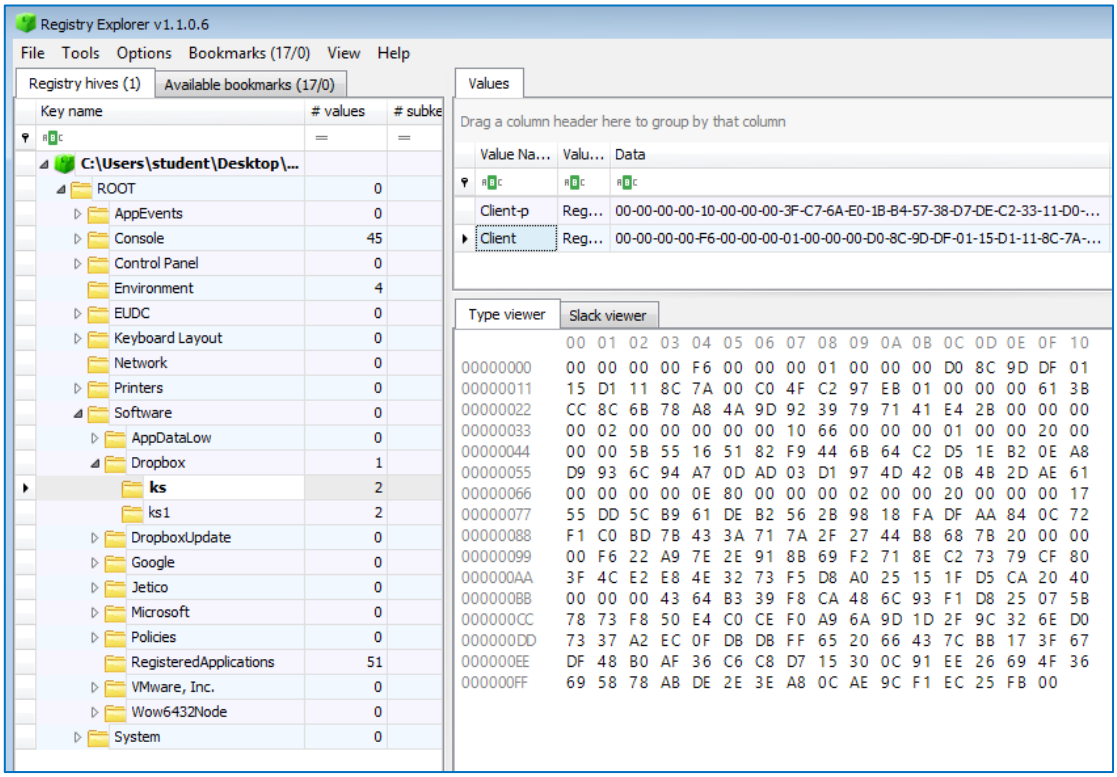


Para conseguir realizar el descifrado deberemos de proporcionarle los siguientes datos:

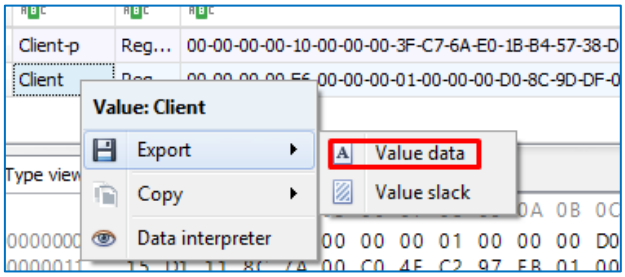
1. **La clave que está cifrada en el registro del usuario (DPAPI data)**Es un data blob de DPAPI, es decir, el contendor que contiene la clave con la que ha sido cifrado Dropbox y se encuentra en el siguiente paso:

- **NTUSER.DAT\Software\Dropbox\ks\Client**

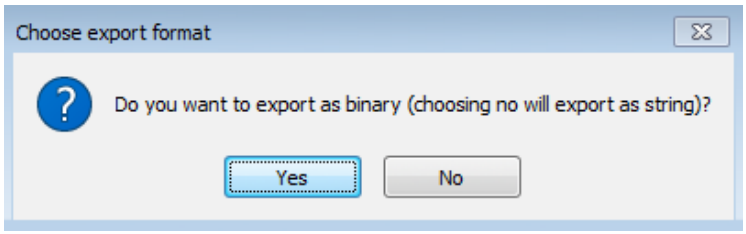
Para obtenerla, tendremos primeramente que extraer mediante FTK Imager el fichero NTUSER.DAT del usuario Pedro y luego utilizaremos la herramienta Registry Explorer



Seleccionamos Client y luego “Export->Value Data”



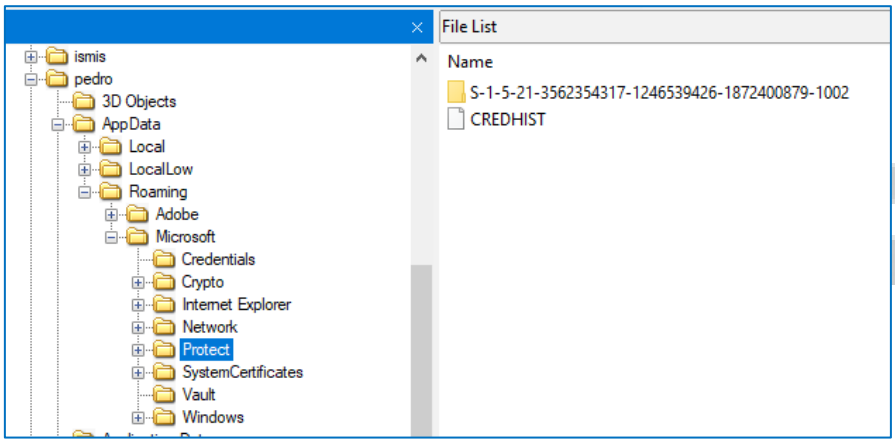
Le decimos que si:



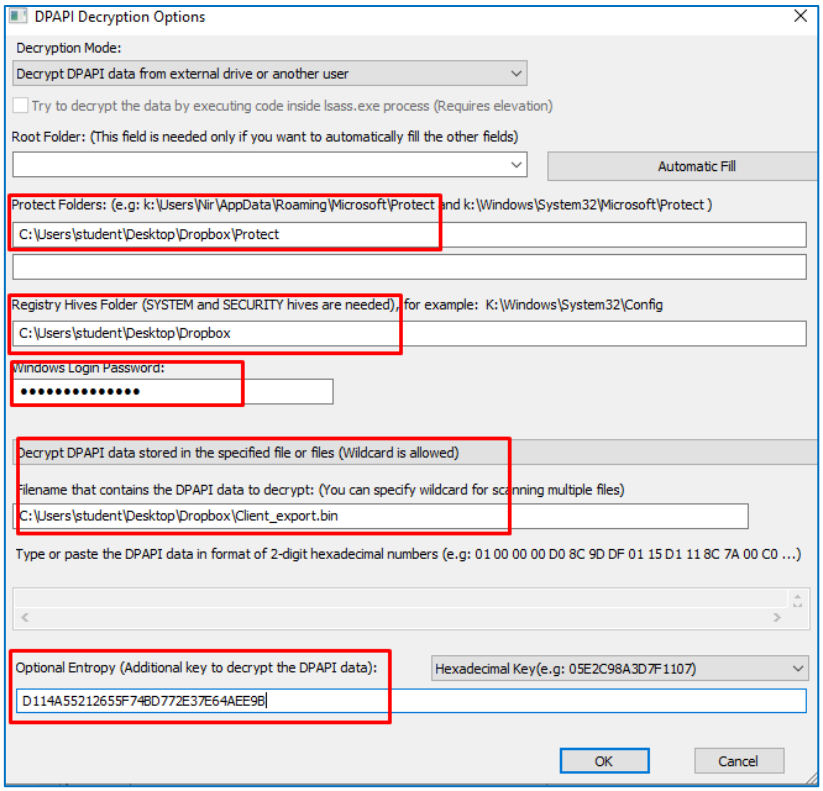
2. **La entropía que la conocemos: D114A55212655F74BD772E37E64AEE9B**
3. **Las credenciales de acceso a Windows del usuario en cuestión. Para esta demo utilizaremos las del usuario Pedro: Microsoft2018!**
4. **Los registros SYSTEM y SECURITY**
5. **Carpeta Protect:**

Dentro del protect folder se encuentran las DPAPI master keys junto con su histórico.

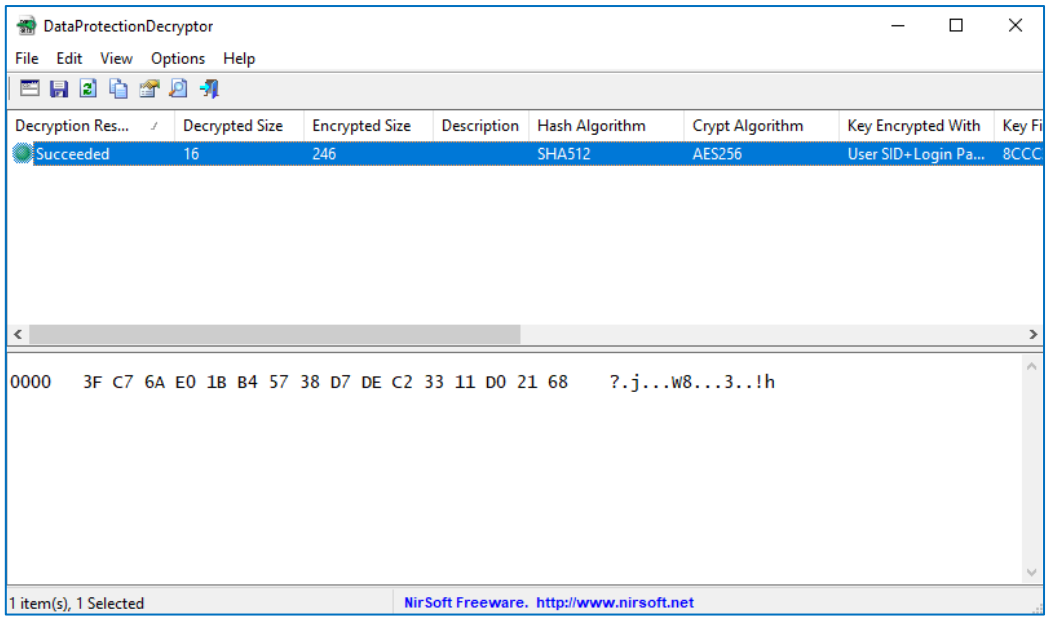
- **\Users\Pedro\AppData\Roaming\Microsoft**



Con todos estos ficheros, simplemente tenemos que introducirlos en DataProtectionDecryptor:

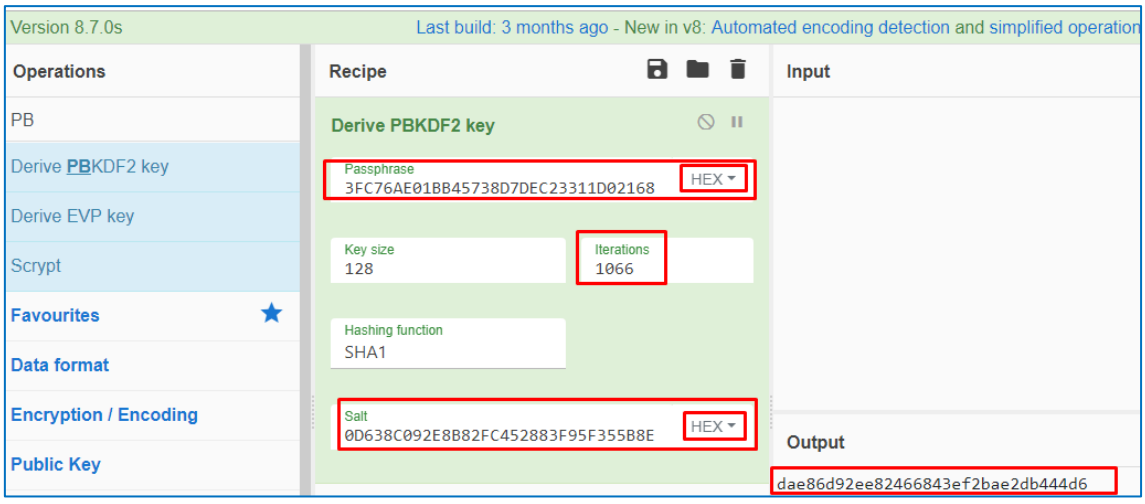

DPAPI Decryption Options
Decryption Mode:
Decrypt DPAPI data from external drive or another user
Try to decrypt the data by executing code inside lsass.exe process (Requires elevation)
Root Folder: (This field is needed only if you want to automatically fill the other fields)
Automatic Fill
Protect Folders: (e.g: k:\Users\Nir\AppData\Roaming\Microsoft\Protect and k:\Windows\System32\Microsoft\Protect)
C:\Users\student\Desktop\Dropbox\Protect
Registry Hives Folder (SYSTEM and SECURITY hives are needed), for example: K:\Windows\System32\Config
C:\Users\student\Desktop\Dropbox
Windows Login Password:
Decrypt DPAPI data stored in the specified file or files (Wildcard is allowed)
Filename that contains the DPAPI data to decrypt: (You can specify wildcard for scanning multiple files)
C:\Users\student\Desktop\Dropbox\Client_export.bin
Type or paste the DPAPI data in format of 2-digit hexadecimal numbers (e.g: 01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0 ...)
Optional Entropy (Additional key to decrypt the DPAPI data):
Hexadecimal Key(e.g: 05E2C98A3D7F1107)
D114A55212655F74BD772E37E64AEE9B
OK
Cancel

Cuando se produzca el cifrado de manera satisfactoria, aparecerá en verde y el mensaje de "Succeeded". El campo de abajo es clave que deberemos usar la función PBKDF para conseguir la clave final:



La clave es 3F C7 6A E0 1B B4 57 38 D7 DE C2 33 11 D0 21 68. A esta clave, la llamaremos clave primaria. Ahora abrimos CyberChef que lo tenemos en el Escritorio y configuramos:

- **Derive PBKDF2, junto con las 1066 iteraciones y la salt 0D638C092E8B82FC452883F95F355B8E en HEX**
- **Insertamos previamente obtenida como Passphrase en HEX**



Finalmente obtenemos:

- **DAE86D92EE82466843EF2BAE2DB444D6**

El siguiente paso, es descifrar la base de datos con clave obtenida. Para ello utilizaremos una versión especial de SQLITE que soporta cifrado y ejecutaremos el siguiente comando sobre la base datos que previamente hemos extraído con FTK Imager:

sqlite-dbx-win64.exe -key XXXXX bbdd.dbx ".backup bbdd.db"

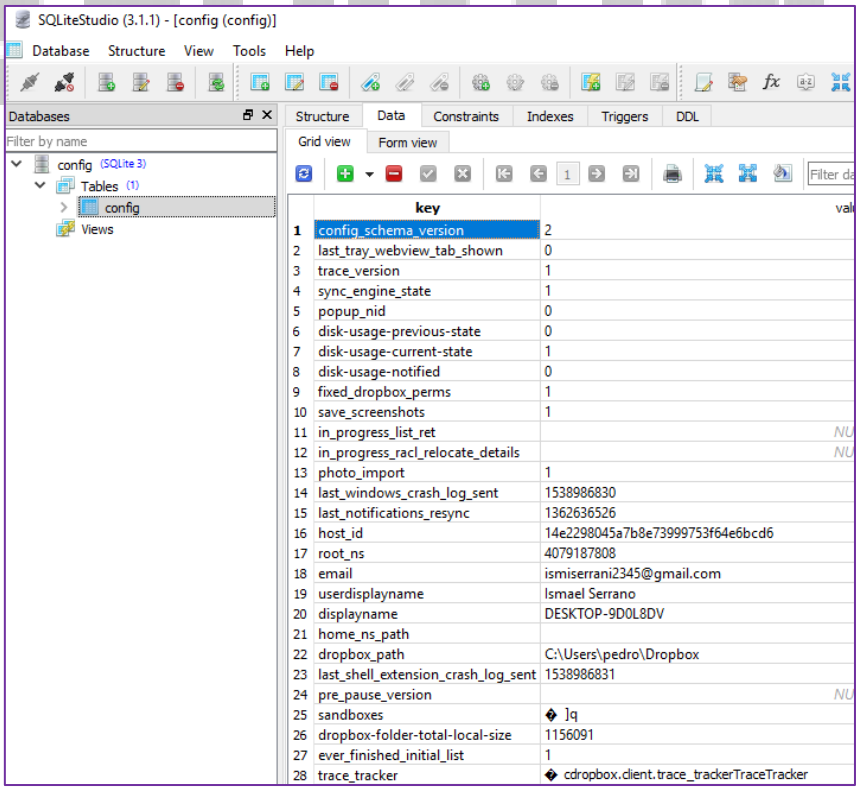
```
C:\Users\student\Desktop\Dropbox>sqlite-dbx-win64.exe -key DAE86D92EE82466843EF2BAE2DB444D6 config.dbx ".backup config.d
b"

C:\Users\student\Desktop\Dropbox>
```

Las bases de datos más relevantes que encontramos de Dropbox son las siguientes:

CONFIG.DBX

Contiene la configuración de la cuenta sincronizada en el equipo y los datos de estos, algunos de los campos interesantes de esta tabla son:

- **Email: dirección de email de la cuenta registrada.**
- **Userdisplayname: nombre del usuario de la cuenta**
- **dropbox_path: dirección donde se encuentra la carpeta de Dropbox en el equipo.**
- **Host_id: hash de autenticación que usa la aplicación de escritorio para autenticarse en la nube. Este hash no cambia al menos que se revoque desde la página web.**
- **Root_ns: identificador del usuario. Este veremos que en la base de datos Filecache.db será utilizado**



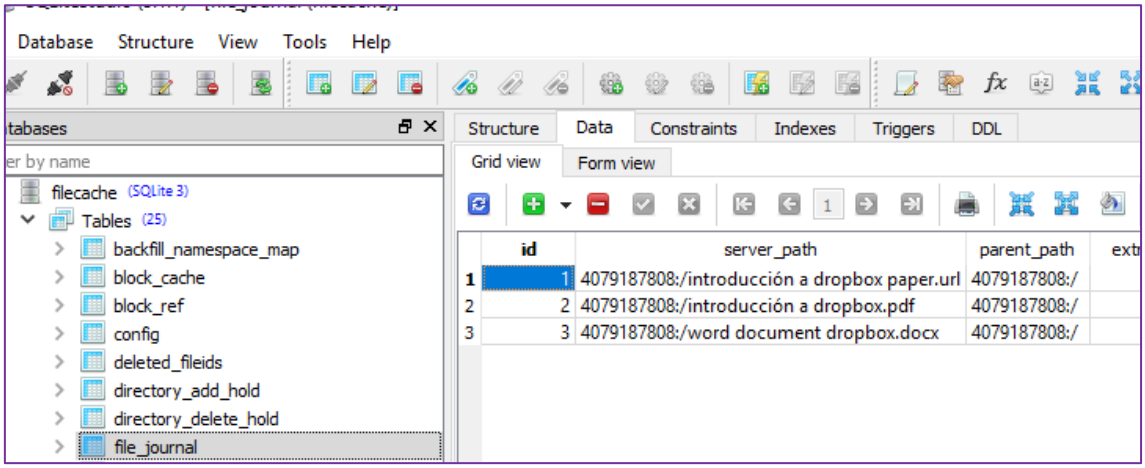
FILECACHE.DB

En esta base de datos, encontraremos información de todos los ficheros y carpetas que están sincronizadas con Dropbox, así como información de estas. Gracias a esta base de datos obtendremos un registro de los ficheros y de lo que ha ocurrido con estos, podremos seguir el rastro incluso de aquellos que no están configurados para ser sincronizados en el equipo. Dentro de esta base de datos encontraremos las siguientes tablas más importantes:

- File_journal: tenemos información de todos los ficheros de Dropbox y de las carpetas de este.

La tabla **File_journal** es la que más información nos dará de los ficheros, así como algunos de sus campos especiales:

- Server_path: la ruta del servidor donde está alojado el archivo. Los ficheros van precedidos por el host_id del cliente, este identificador podemos ver que está también registrado en la tabla "config" en el registro "root_ns"
- local_sjid : la versión del archivo. Como sabemos, Dropbox cuando hacemos modificaciones sobre un fichero, nos va almacenando las versiones de estos, este número de versión es el que está almacenado en este campo
- local_mtime: fecha de modificación del fichero (formato epoch)
- local_ctime fecha de creacción del fichero (formato epoch)



Seguimos enumerando las tablas dentro de la base de datos **Filecache.db**:

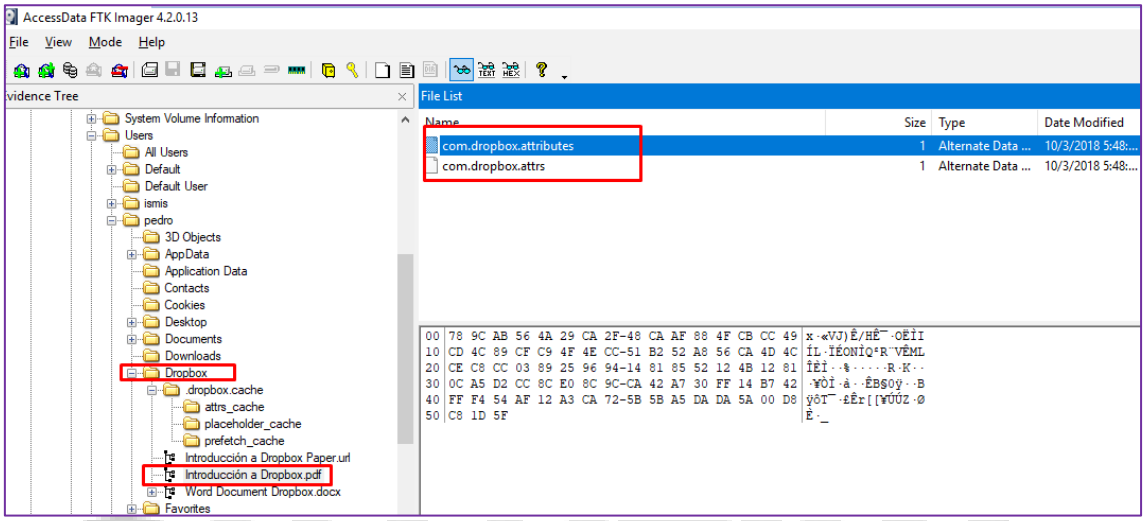
- block_cache: almacena el hash de todos los archivos y directorios de Dropbox
- block_ref : en esta base de datos podemos relacionar el identificador del hash de la tabla block_cache con el identificador del fichero en la tabla file_journal
- mount_table: las carpetas compartidas de Dropbox
- deleted_fields: los archivos que han sido eliminados de Dropbox
    - date_added: la fecha en la que se ha añadido la entrada en la base de datos, que corresponde la fecha en la que se ha eliminado el fichero

Ver video: 001/MÓD.7 - Descifrado SQLITE Dropbox

ALTERNATE DATA STEAM EN DROPBOX

Tal y como vemos en el siguiente enlace, todos los ficheros que hay en la carpeta de sincronización de Dropbox, tienen un Alternate Data Stream. Este hecho es muy importante, porque podríamos trazar que ficheros han estado en Dropbox si los encontrásemos en el sistema de archivos:

https://blog.didierstevens.com/2017/01/30/quickpost-dropbox-alternate-data-streams/



En la imagen anterior, aparecen dos ADS:

- com.dropbox.atributtes
- com.dropbox.attrs

El análisis del com.dropbox.atributtes tiene un header conocido, tal y como indica el análisis efectuado en la web anterior obteniendo el identificador propio de Dropbox de la maquina en el que estuvo.

Es muy importante saber que para todas las bases de datos que hemos visto en formato SQLite, en caso de que fuesen borradas del sistema de archivos, se podría realizar una recuperación mediante técnicas de carving, tal y como hemos visto en módulos anteriores y en especial se podría utilizar Photorec.