

## Práctica 1

# Análisis forense en la nube

---

Jose Almirón López

09 de Abril del 2024

## Tabla de contenidos

<b>A Taxonomy of Cloud Endpoint Forensic Tools</b>	<b>3</b>
¿Qué es el análisis forense de la nube?	3
¿Cuáles son las fuentes de evidencias digitales que nos encontramos específicamente cuando trabajamos en la nube?	3
¿Qué posibilidades nos ofrece explotar las API que nos ofrecen los proveedores de servicios en la nube? Explica los metadatos que se pueden obtener haciendo uso de las API.	4
Enumera el software cliente más utilizado a la hora de acceder a servicios en la nube (ver tablas 1,2 y 3)	5
<b>Onedrive</b>	<b>5</b>
Identificación donde se instala y su configuración	5
Localiza dónde se sitúan las carpetas que se sincroniza en la nube	6
Encontrar los metadatos generan y qué información podemos extraer de ellos	7
<b>Google Drive</b>	<b>9</b>
Identificación donde se instala y su configuración	9
Localiza dónde se sitúan las carpetas que se sincroniza en la nube	10
Encontrar los metadatos generan y qué información podemos extraer de ellos	11
<b>Dropbox</b>	<b>12</b>
Identificación donde se instala y su configuración	12
Localiza dónde se sitúan las carpetas que se sincroniza en la nube	13
Encontrar los metadatos generan y qué información podemos extraer de ellos	13

## A Taxonomy of Cloud Endpoint Forensic Tools

### ¿Qué es el análisis forense de la nube?

El análisis forense de la nube, también conocido como cloud forensics, es la disciplina que aplica los principios de la ciencia forense digital en el ámbito de la computación en la nube. Se centra en la recolección, preservación, examen e interpretación de evidencia digital relacionada con eventos pasados dentro de entornos de computación en la nube. Esto implica la identificación y extracción de datos relevantes almacenados tanto en dispositivos finales (endpoint devices) como en los servidores de los proveedores de servicios en la nube.


El análisis forense de la nube enfrenta desafíos particulares debido a la naturaleza distribuida, multi-jurisdiccional y multiinquilino de la nube. Los investigadores forenses necesitan emplear herramientas especializadas para acceder, recolectar y analizar datos en entornos de nube de manera forense, manteniendo la integridad y autenticidad de la evidencia recopilada.

Este campo, en constante evolución, demanda un enfoque híbrido que combine diversas técnicas forenses, como la forense virtual, de red y en vivo, para abordar los desafíos únicos que presenta la computación en la nube en términos de adquisición y análisis de evidencia digital [T5].

### ¿Cuáles son las fuentes de evidencias digitales que nos encontramos específicamente cuando trabajamos en la nube?

Cuando nos adentramos en el análisis forense de la nube, nos encontramos con diversas fuentes de evidencia digital que pueden residir tanto en los dispositivos finales (endpoint devices) como en los servidores de los proveedores de servicios en la nube. Aquí algunas de las fuentes específicas de evidencia digital:


1. **Archivos y carpetas sincronizados:** Estos son elementos que se generan en el dispositivo local cuando se utiliza software cliente para interactuar con el servidor en la nube. Contienen datos pertinentes que pueden ser relevantes para la investigación forense.
2. **Papelera de reciclaje:** La papelera de reciclaje es un componente crucial en la búsqueda de datos eliminados durante una investigación forense. Incluso después de la eliminación de datos sincronizados, es posible que aún se puedan recuperar datos relacionados con la nube.

- 
3. **Metadatos de archivos:** Los metadatos de los archivos, tales como tamaño, fecha y hora de creación, versión, tipo de archivo, entre otros, pueden proporcionar información valiosa para el análisis forense.
  4. **Historial del navegador y caché:** La interacción con servicios en la nube a través de navegadores web o aplicaciones móviles genera registros e información que pueden identificar al usuario y brindar detalles sobre sus actividades.
  5. **Archivos de registro de eventos:** Durante la interacción con los servicios en la nube, se generan archivos de registro de eventos que pueden contener datos relevantes para la investigación forense.

¿Qué posibilidades nos ofrece explotar las API que nos ofrecen los proveedores de servicios en la nube? Explica los metadatos que se pueden obtener haciendo uso de las API.

Al aprovechar las API (Interfaces de Programación de Aplicaciones) proporcionadas por los proveedores de servicios en la nube, los investigadores forenses pueden acceder a una amplia variedad de datos y metadatos cruciales para las investigaciones en entornos de computación en la nube. Aquí hay algunas de las capacidades que ofrecen las API de la nube:

1. **Acceso directo a datos en la nube:** Las API permiten a los investigadores acceder directamente a los datos almacenados en los servidores de los proveedores de servicios en la nube, simplificando la recopilación de evidencia digital sin la necesidad de acceder físicamente a los dispositivos finales.
2. **Extracción de metadatos:** Los metadatos son datos que describen otros datos y ofrecen información crucial sobre los archivos y carpetas almacenados en la nube. Mediante el uso de las API, es posible obtener metadatos tales como:
  - Nombre del archivo
  - Tamaño del archivo
  - Fecha y hora de creación
  - Versión del archivo
  - Tipo de archivo
  - Ruta remota del archivo
  - Ruta de descarga del archivo
  - Historial de revisiones
  - Valores hash
  - Estampillas de tiempo



Enumera el software cliente más utilizado a la hora de acceder a servicios en la nube (ver tablas 1,2 y 3)

Según las tablas proporcionadas en el documento "A Taxonomy of Cloud Forensic Tools", algunos de los software cliente más utilizados para acceder a servicios en la nube incluyen:

Navegadores web:

- Internet Explorer
- Mozilla Firefox
- Google Chrome

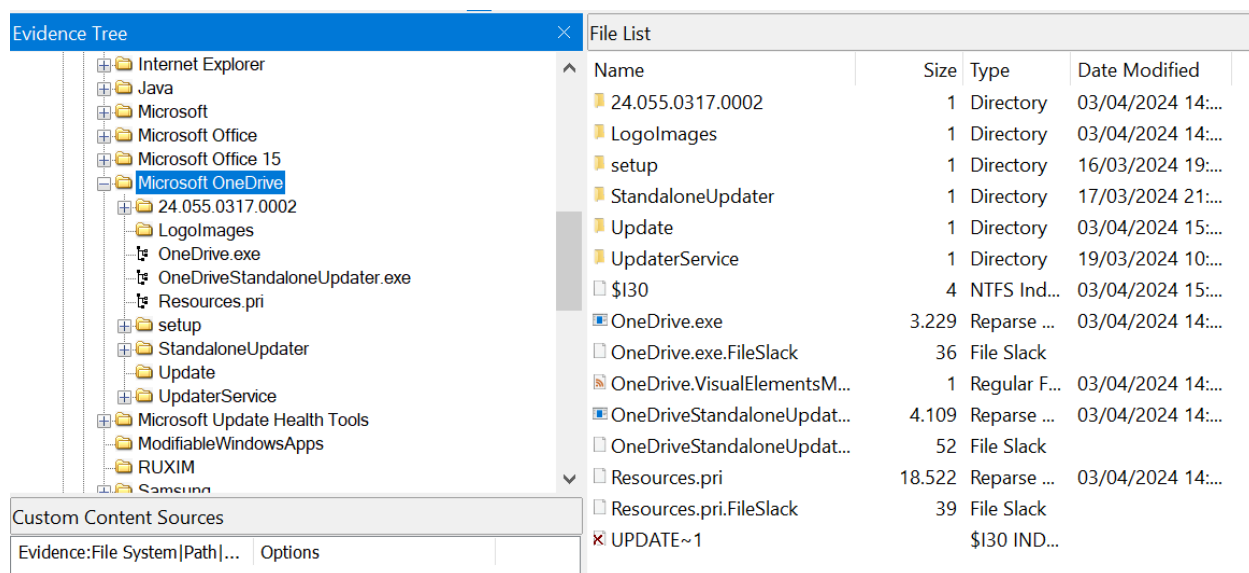
Clientes de servicios en la nube:

- Dropbox Client
- Google Drive Client
- OneDrive Client
- Amazon Cloud Drive Client
- Mega v1 App
- hubiC Client
- Evernote Client
- ownCloud Sync Client
- IDrive Client
- Mega Cloud Drive

## Onedrive

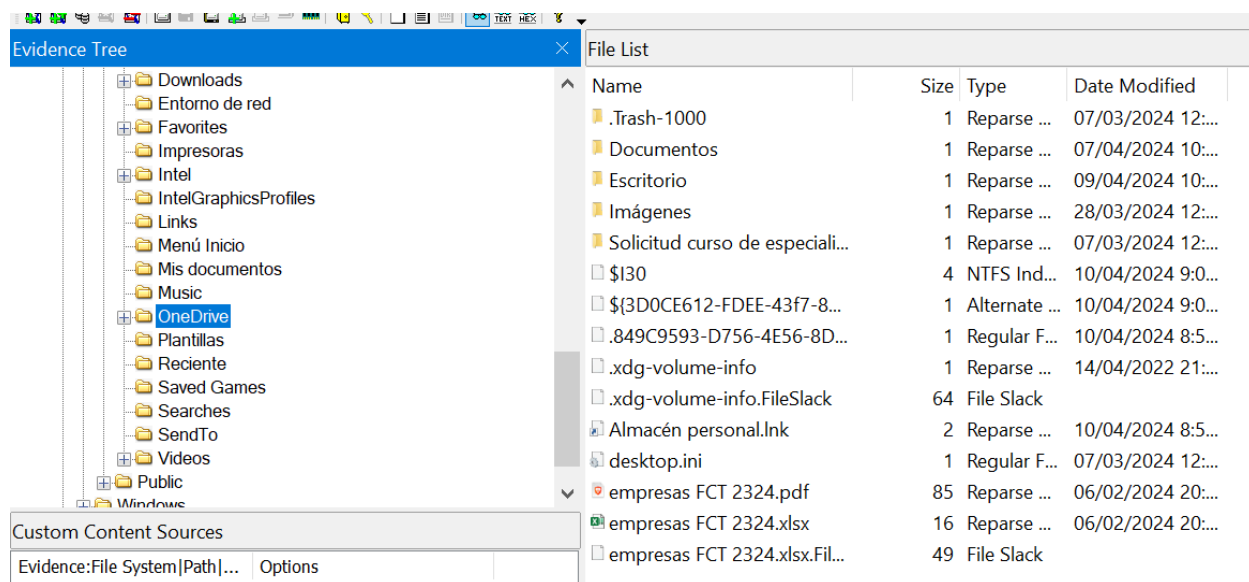
### Identificación donde se instala y su configuración

En sistemas operativos Windows, OneDrive se instala por defecto como parte del sistema operativo y su carpeta de instalación está ubicada en "**C:\Program Files\Microsoft OneDrive**". La configuración de OneDrive se puede acceder y modificar a través del icono de OneDrive en la barra de tareas o en la configuración del sistema.



## Localiza dónde se sitúan las carpetas que se sincroniza en la nube

En sistemas Windows, las carpetas que se sincronizan con la nube a través de OneDrive generalmente se encuentran en la carpeta del usuario, dentro de la carpeta "OneDrive", cuya ruta completa sería "**C:\Users[nombre de usuario]\OneDrive**".



## Encontrar los metadatos generan y qué información podemos extraer de ellos

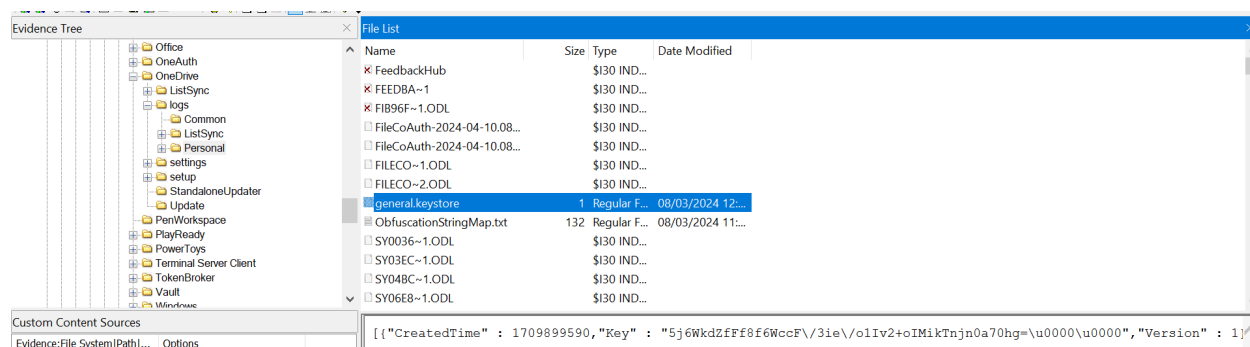
Para encontrar los metadatos generados en los registros de OneDrive y la información que podemos extraer de ellos, podemos considerar lo siguiente:

1. **Metadatos en los registros de OneDrive:** Los metadatos en los registros de OneDrive pueden incluir información como marcas de tiempo, nombres de archivos, rutas de archivos, nombres de funciones, parámetros de funciones, versiones de OneDrive y del sistema operativo, entre otros. Estos metadatos proporcionan detalles sobre las acciones realizadas en OneDrive, como subidas, descargas, sincronizaciones, enlaces de cuentas, etc.
2. **Información extraíble de los metadatos:**
  - **Marcas de tiempo:** Nos indican cuándo ocurrieron ciertos eventos en OneDrive, lo que puede ser crucial para reconstruir secuencias de eventos.
  - **Nombres de archivos y rutas:** Nos permiten rastrear qué archivos se manipularon y dónde se almacenaron.
  - **Nombres de funciones y parámetros:** Proporcionan información sobre las operaciones realizadas en OneDrive, lo que puede ayudar a comprender las acciones específicas llevadas a cabo.
  - **Versiones de OneDrive y del sistema operativo:** Ayudan a contextualizar los eventos registrados y a asegurar la compatibilidad con las versiones de software utilizadas.
3. **Proceso de extracción de información:** Para extraer información de los metadatos en los registros de OneDrive, es necesario desobfuscar las cadenas obfuscatas, interpretar los datos estructurados en los archivos .odl y .odlgz, y analizar los registros de funciones y archivos para reconstruir las actividades realizadas en OneDrive.

Además de los registros odl, debería haber un archivo llamado ObfuscationStringMap.txt. Este archivo es necesario para despejar cadenas. Por lo general, solo hay uno de estos archivos por instalación de OneDrive, ya sea en la carpeta Personal o Empresarial1, pero todos los registros odl lo utilizan.

En las versiones más recientes desde abril de 2022, es posible que no haya un archivo ObfuscationStringMap.txt. En lugar de eso, ahora necesitas el general.keystore(en la misma ubicación) para despejar las cadenas.

Estos ficheros los encontraremos en el directorio de log en la ruta “**C:\Users[nombre de usuario]\AppData\Local\Microsoft\OneDrive\logs**”, concretamente en Personal, podremos exportar este directorio para trabajar con un script a continuación.



He encontrado un script en un repositorio de [GitHub](#) que nos permite extraer toda esta información y guardarla en un archivo CSV. Esto facilita el manejo de los datos, ya que podemos utilizar herramientas de análisis y visualización para examinar la información de manera más efectiva

***python3 odl.py -o ~D:\onedrive.csv C:\Users\jose\Desktop\Personal***

```
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0939.1508.167.aod1
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0939.1508.179.aod1
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0939.1508.191.aod1
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0939.1508.203.aod1
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0940.1508.215.aod1
File is empty, file size is 0 bytes
Searching C:\Users\jose\OneDrive\Escritorio\Personal\SyncEngine-2024-04-10.0955.1508.263.aod1
File is empty, file size is 0 bytes
Finished processing files, output is at D:\onedrive.csv
D:\VirtualBox\VMs\Carpetas-Compartidas\OneDrive\
```

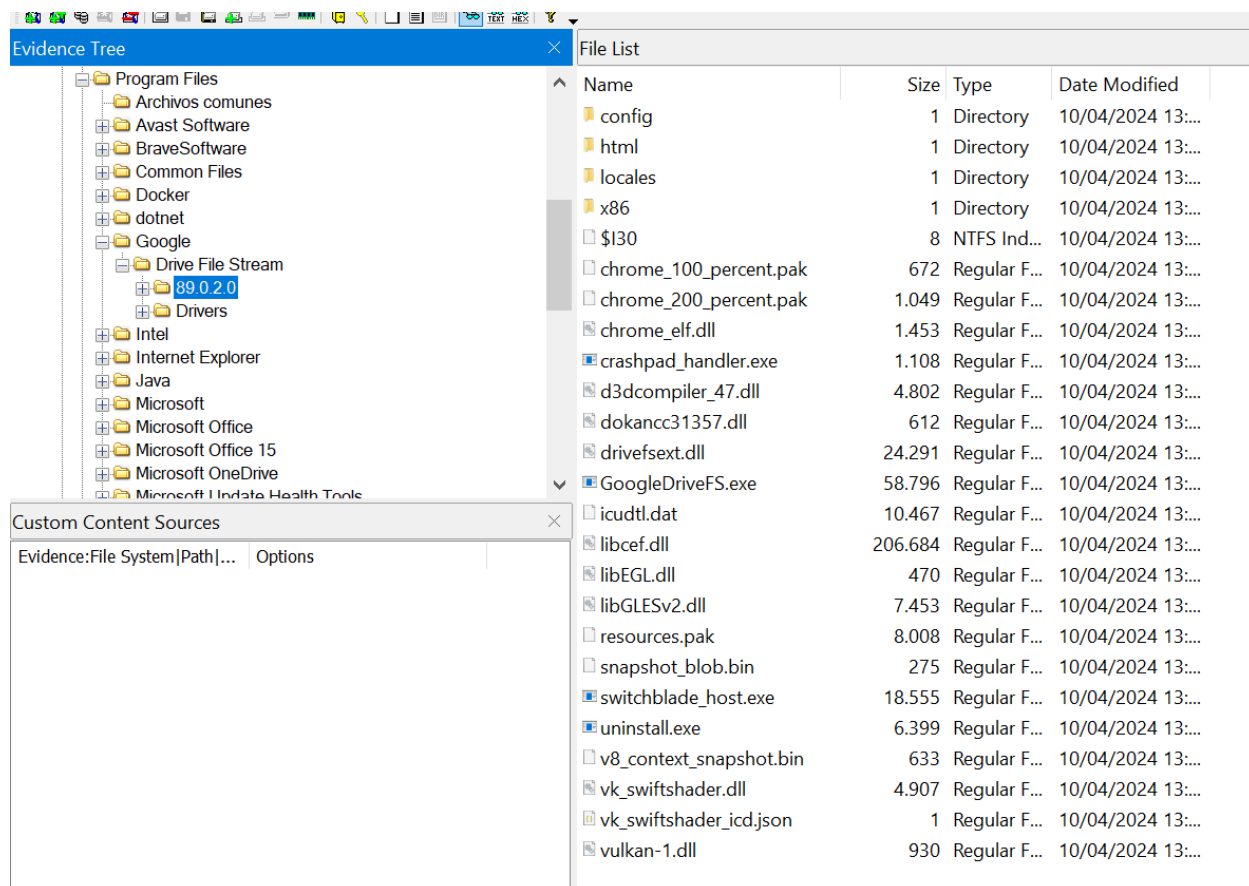


```
onedrive.csv
D:\> onedrive.csv
1  Filename,File_Index,Timestamp,Code_File,Function,Params_Decoded
2
3  SyncEngine-2024-03-08.0847.1928.2.odlsent,12,2024-03-08 08:47:14.681000,WorkerThreadPool.cpp,WorkerThreadPool::AddThread,Diagnostics
4
5  SyncEngine-2024-03-08.0847.1928.2.odlsent,15,2024-03-08 08:47:14.681000,Realizer.cpp,Realizer::ProcessChanges,LC_PERSIST_SYNC_TOKEN 15
6
7  SyncEngine-2024-03-08.0847.1928.2.odlsent,16,2024-03-08 08:47:14.681000,WorkerThreadPool.cpp,WorkerThreadPool::WorkerMainLoop,Diagnostics
8
9  SyncEngine-2024-03-08.0847.1928.2.odlsent,18,2024-03-08 08:47:14.682000,SyncProgressAudit.cpp,SyncProgressDiagnosticInfo::SendDiagnosticInfo,"[
10
11  SyncEngine-2024-03-08.0847.1928.2.odlsent,19,2024-03-08 08:47:14.682000,Diagnostics.cpp,Diagnostics::ReportDiagnosticInfoWorker,"['sync_progre
12
13  SyncEngine-2024-03-08.0847.1928.2.odlsent,20,2024-03-08 08:47:14.682000,PersistSyncToken.cpp,PersistSyncToken::Process,"['C27487A79BB0ABF4!106'
14
15  SyncEngine-2024-03-08.0847.1928.2.odlsent,21,2024-03-08 08:47:14.682000,LocalChange.cpp,LocalChange::SendProcessResultTelemetry,"['LocalChange'
16
17  SyncEngine-2024-03-08.0847.1928.2.odlsent,22,2024-03-08 08:47:14.683000,Realizer.cpp,Realizer::ProcessChanges,LC_SYNC_COMPLETE 7
18
19  SyncEngine-2024-03-08.0847.1928.2.odlsent,23,2024-03-08 08:47:14.683000,SyncComplete.cpp,SyncComplete::Process,C27487A79BB0ABF4!106
20
21  SyncEngine-2024-03-08.0847.1928.2.odlsent,35,2024-03-08 08:47:14.684000,LocalChange.cpp,LocalChange::SendProcessResultTelemetry,"['LocalChange'
22
23  SyncEngine-2024-03-08.0847.1928.2.odlsent,36,2024-03-08 08:47:14.684000,ScenarioTracking.cpp,ScenarioTracking::ReportUnrecordedScenario,"['Finc
24
```

## Google Drive

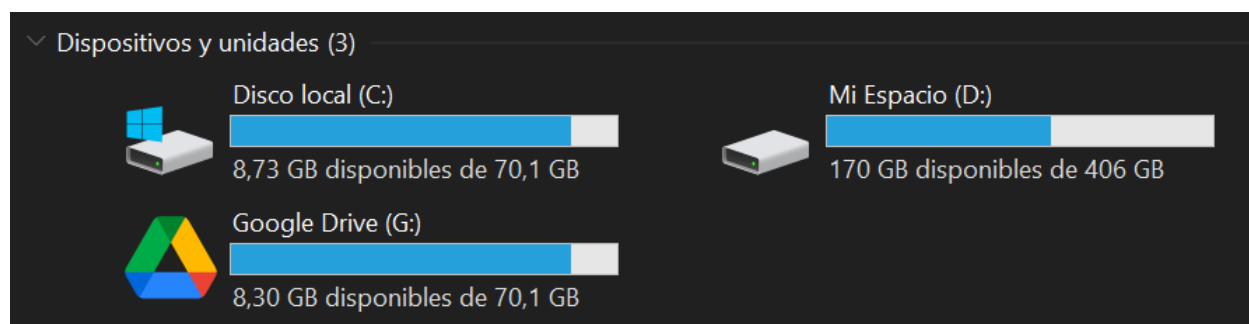
### Identificación donde se instala y su configuración

En sistemas Windows, el cliente de Google Drive se instala por defecto en la siguiente ruta: **"C:\Users[Nombre de usuario]\Program Files\Google\Drive Stream[versión]".** La configuración del cliente de Google Drive se realiza a través de la aplicación. En Windows, puedes acceder a la configuración haciendo clic en el icono de Google Drive en la bandeja del sistema y seleccionando **"Preferencias"**



## Localiza dónde se sitúan las carpetas que se sincroniza en la nube

En un sistema Windows, cuando se sincronizan las carpetas en la nube a través de Google Drive, se agrega una nueva unidad de almacenamiento a nuestros dispositivos. Esta unidad sincroniza los archivos del usuario con el servicio en la nube de Google Drive

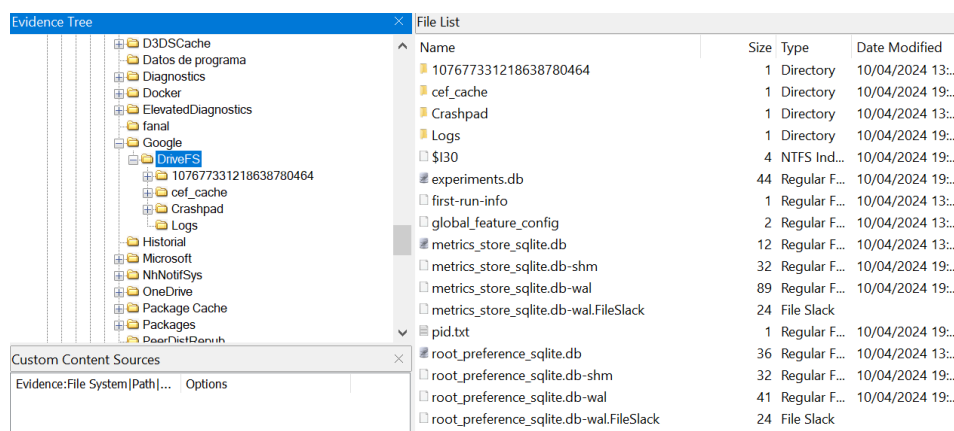


Encontrar los metadatos generan y qué información podemos extraer de ellos

Por defecto, los archivos residuales generados por Google Drive se guardan en la siguiente ruta:  
**C:\Usuarios\%user%\AppData\Local\Google\DriveFS.**

Esta carpeta almacena una variedad de subcarpetas y bases de datos que son fundamentales para almacenar información relevante sobre las actividades del usuario en la aplicación. A continuación se enumeran las subcarpetas/archivos más importantes:

- **root\_preference\_sqlite.db:** Esta base de datos guarda información sobre todos los dispositivos que han sido parcial o totalmente respaldados en Google Drive, así como cualquier dispositivo conectado a la computadora mientras la aplicación Google Drive estaba en ejecución. Además, almacena datos relacionados con las raíces (carpetas) sincronizadas con la nube mediante la aplicación de escritorio Google Drive.
- **mirror\_sqlite.db:** En contraste, esta base de datos contiene información sobre todos los elementos, ya sean carpetas raíz, subcarpetas o archivos, que han sido sincronizados con la nube mediante la aplicación de escritorio Google Drive.
- **%user\_acount\_id%\metadata\_sqlite\_db** y **%user\_acount\_id%\mirror\_metadata\_sqlite.db:** Google Drive genera una carpeta única para cada cuenta, identificada por un código único de 21 dígitos. Dentro de esta carpeta, se encuentran las bases de datos mencionadas anteriormente, que guardan información sobre los elementos almacenados en la nube mediante Google Drive, así como datos sobre elementos eliminados y detalles relacionados con la cuenta del usuario.
- **cef\_cache\Caché:** Aquí se encuentran los detalles de la caché recopilados por la aplicación de escritorio Google Drive, organizados en la estructura de caché de Chromium.



The screenshot shows a database management interface with a 'Databases' pane on the left and a 'Structure' pane on the right. The 'Databases' pane shows a tree view of databases, with 'mirror\_metadata\_sqlite (SQLite 3)' expanded to show a list of tables. The 'Structure' pane shows the 'item\_properties' table structure.

	item_stable_id	key	value	value_type
1	102	td-change-id	297	2
2	102	td-active	1	1
3	102	local-title	Ejericicios Resueltos	3
4	102	version-counter	1	2
5	102	td-cache-type	0	2
6	102	td-last-used	0	2
7	304	local-title	indice	3
8	304	version-counter	1	2
9	305	local-title	prastica forense	3
10	305	version-counter	1	2

## Dropbox

### Identificación donde se instala y su configuración

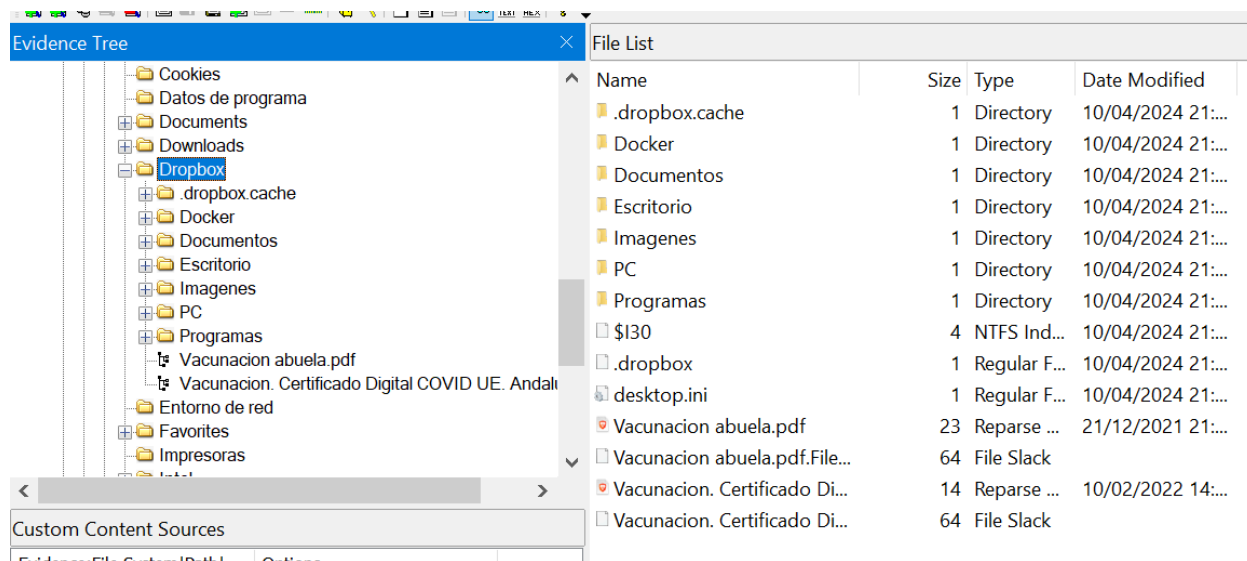
Por lo general, Dropbox se instala en la ruta estándar del disco **C:\Program Files (x86)\Dropbox**. Esta es la ubicación donde se encuentra el archivo ejecutable de la aplicación.

The screenshot shows a file explorer window with an 'Evidence Tree' pane on the left and a 'File List' pane on the right. The 'Evidence Tree' pane shows a tree view of the file system, with 'Program Files (x86)\Dropbox' expanded to show a list of files and folders. The 'File List' pane shows the details of the files and folders in the selected path.

Name	Size	Type	Date Modified
196.4.6900	1	Directory	10/04/2024 21:...
PackageAssets	1	Directory	10/04/2024 21:...
\$I30	4	NTFS Ind...	10/04/2024 21:...
Dropbox.exe	11.281	Regular F...	02/04/2024 11:...
Dropbox.VisualElementsM...	1	Regular F...	01/01/2000
DropboxExt.71.0.dll	559	Regular F...	02/04/2024 11:...
DropboxExt64.71.0.dll	603	Regular F...	02/04/2024 11:...
DropboxUninstaller.exe	224	Regular F...	02/04/2024 11:...
qt.conf	1	Regular F...	01/01/2000
resources.pri	134	Regular F...	02/04/2024 11:...

## Localiza dónde se sitúan las carpetas que se sincroniza en la nube

Las carpetas que se sincronizan con la nube mediante la aplicación de Dropbox suelen ubicarse en el siguiente directorio del sistema de archivos: **C:\Users<nombre de usuario>\Dropbox**. Esta carpeta es utilizada por la aplicación de Dropbox para sincronizar los archivos del usuario con el servicio en la nube de Dropbox.



## Encontrar los metadatos generan y qué información podemos extraer de ellos

Para localizar los metadatos generados por Dropbox en un sistema Windows 10 y extraer información relevante, podemos examinar varios artefactos. Estos archivos suelen estar ubicados en la ruta **C:\Users<nombre de usuario>\AppData\Local\Dropbox**.

1. **Prefetch Files:** Los archivos de Prefetch contienen metadatos sobre las aplicaciones ejecutadas en un sistema Windows. En el caso de Dropbox, el archivo de Prefetch asociado puede ser "DROPBOX.EXE-XXXXXXX.pf" ubicado en "C:\Windows\Prefetch". Estos archivos pueden proporcionar información sobre la ejecución de la aplicación Dropbox en el sistema .
2. **LNK Files:** Los archivos LNK (accesos directos) pueden revelar información sobre la ubicación de los archivos ejecutables de Dropbox en el sistema. Por ejemplo, el acceso directo "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" puede indicar la ubicación del ejecutable de Dropbox en el sistema .

### 3. Archivos de Configuración y Bases de Datos:

- **"info.json"** en "C:\Users<username>\AppData\Local\Dropbox": Este archivo almacena un UID que puede ayudar a identificar qué dispositivo cargó un archivo específico en Dropbox .
- **"config.dbx"** en "C:\Users<username>\AppData\Local\Dropbox\instance1": Esta base de datos contiene información como el correo electrónico de la cuenta de Dropbox del usuario .
- **"filecache.dbx"** en "C:\Users<username>\AppData\Local\Dropbox\instance1": Esta base de datos almacena información sobre los archivos sincronizados con la cuenta de Dropbox del usuario .

4. **Event Logs:** Los registros de eventos de Windows, como "Application.evtx", pueden proporcionar información sobre la instalación y desinstalación de la aplicación Dropbox. Por ejemplo, el Event ID 1034 indica que Windows Installer eliminó un producto relacionado con Dropbox .

The screenshot displays a forensic analysis tool interface. On the left, the 'Evidence Tree' shows a directory structure with 'Dropbox' selected. Below it, the 'Custom Content Sources' pane shows 'Evidence:File System|Path|...' and 'Options'. On the right, the 'File List' pane shows a table of files and directories.

Name	Size	Type	Date Modified
avatar_cache	1	Directory	10/04/2024 21:...
Crashpad	1	Directory	10/04/2024 21:...
events	1	Directory	10/04/2024 21:...
instance1	1	Directory	11/04/2024 13:...
instance_db	1	Directory	10/04/2024 21:...
logs	1	Directory	10/04/2024 21:...
machine_storage	1	Directory	10/04/2024 21:...
metrics	1	Directory	10/04/2024 21:...
QuitReports	1	Directory	11/04/2024 13:...
\$I30	4	NTFS Ind...	11/04/2024 13:...
apex.sqlite3	4	Regular F...	10/04/2024 21:...
apex.sqlite3-shm	32	Regular F...	11/04/2024 13:...
apex.sqlite3-wal	552	Regular F...	11/04/2024 13:...
apex.sqlite3-wal.FileSlack	25	File Slack	
host.db	1	Regular F...	11/04/2024 13:...
host.dbx	1	Regular F...	11/04/2024 13:...
info.json	1	Regular F...	11/04/2024 13:...
ksmigrated.dbx	1	Regular F...	10/04/2024 21:...
ksmigrated_config.dbx	1	Regular F...	10/04/2024 21:...
ksmigrated_variant.dbx	1	Regular F...	10/04/2024 21:...
unlink.db	1	Regular F...	11/04/2024 13:...
unlink.db	1	Regular F...	10/04/2024 21:...
UNLINK~1.DB-		\$I30 IND...	