Name: Ghulam Abbas

Roll No: BS DFCS/Fa-22/030

Assignment submitted to: -

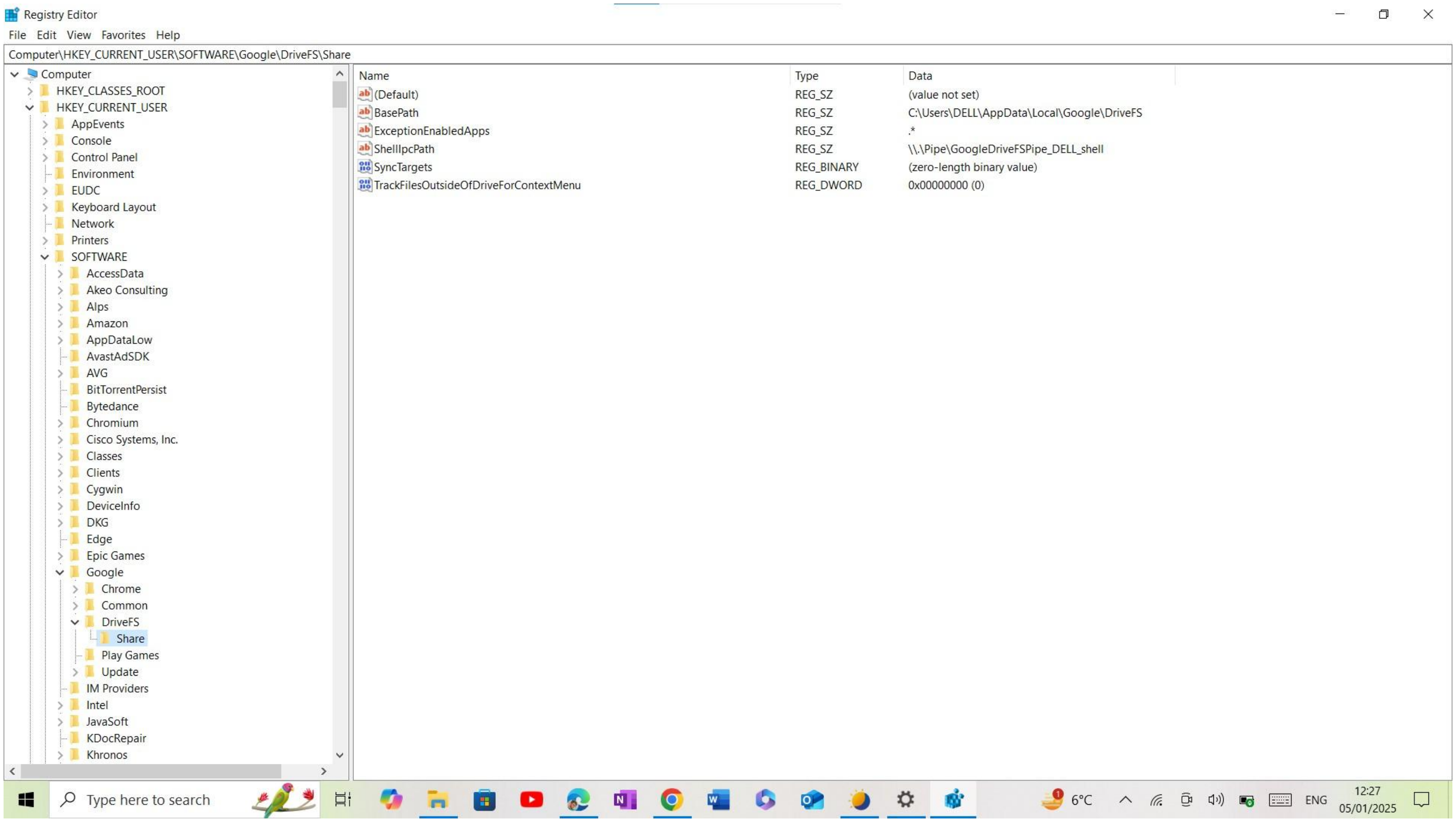
Ms. Fatima

Assignment is: Assignment is: Create Artifacts and Set Log files for Cloud Storage Services i.e. Google Drive that may provide relevant information for Forensic Investigation

1. Artifacts created during the installation process

I. GoogleDriveFS Registry Path

- **Keys related to the installation, such as:**
  `HKCU\Software\Google\DriveFS`

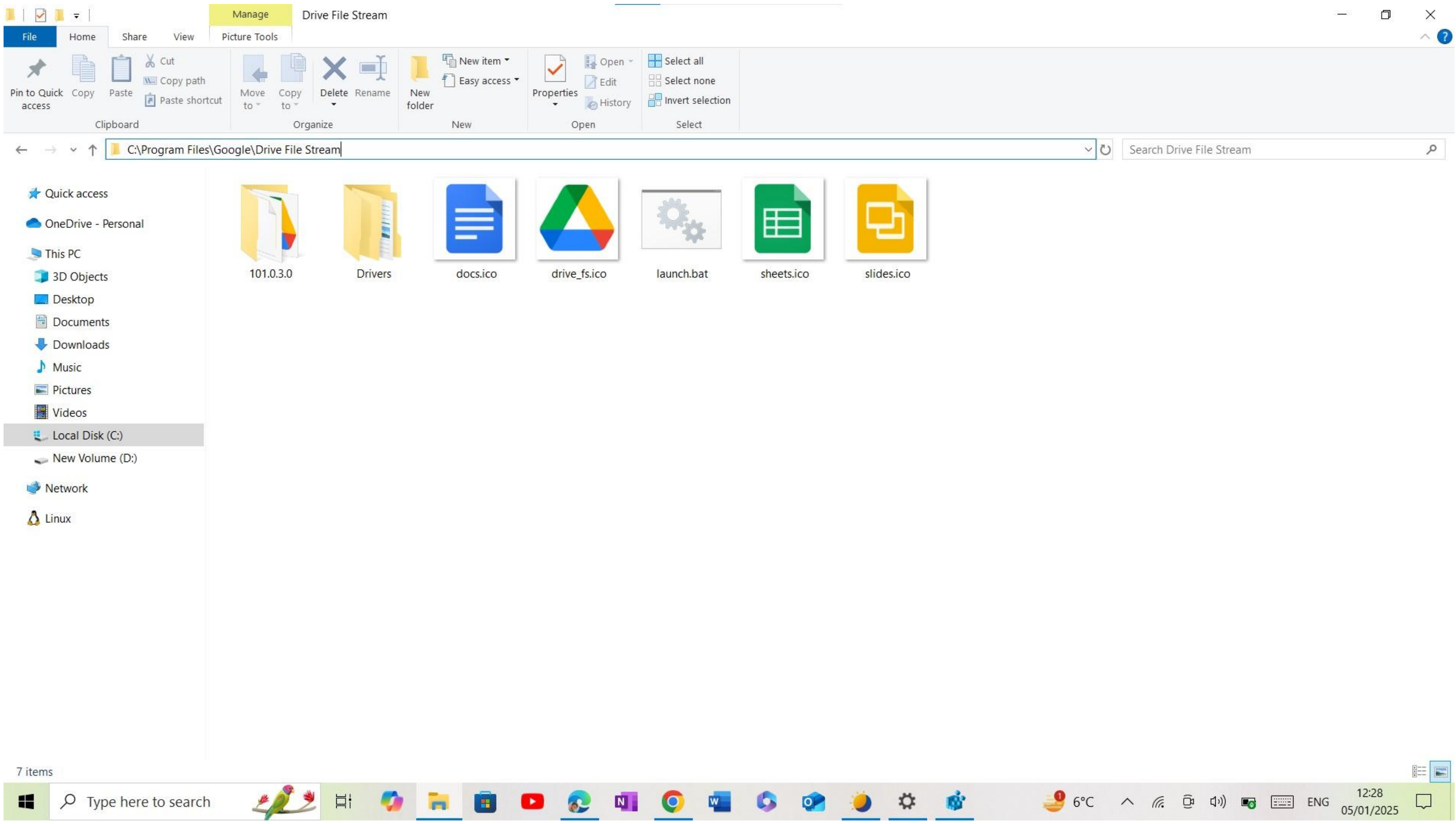


Computer\HKEY_CURRENT_USER\SOFTWARE\Google\DriveFS\Share

Name	Type	Data
(Default)	REG_SZ	(value not set)
BasePath	REG_SZ	C:\Users\DELL\AppData\Local\Google\DriveFS
ExceptionEnabledApps	REG_SZ	.*
ShellIpcPath	REG_SZ	\\.\Pipe\GoogleDriveFSPipe_DELL_shell
SyncTargets	REG_BINARY	(zero-length binary value)
TrackFilesOutsideOfDriveForContextMenu	REG_DWORD	0x00000000 (0)

II. Directory Path

- Default installation directory, e.g.,
  C:\Program Files\Google\Drive
- Executable files: drive.exe, googledrivesync.exe



Drive File Stream

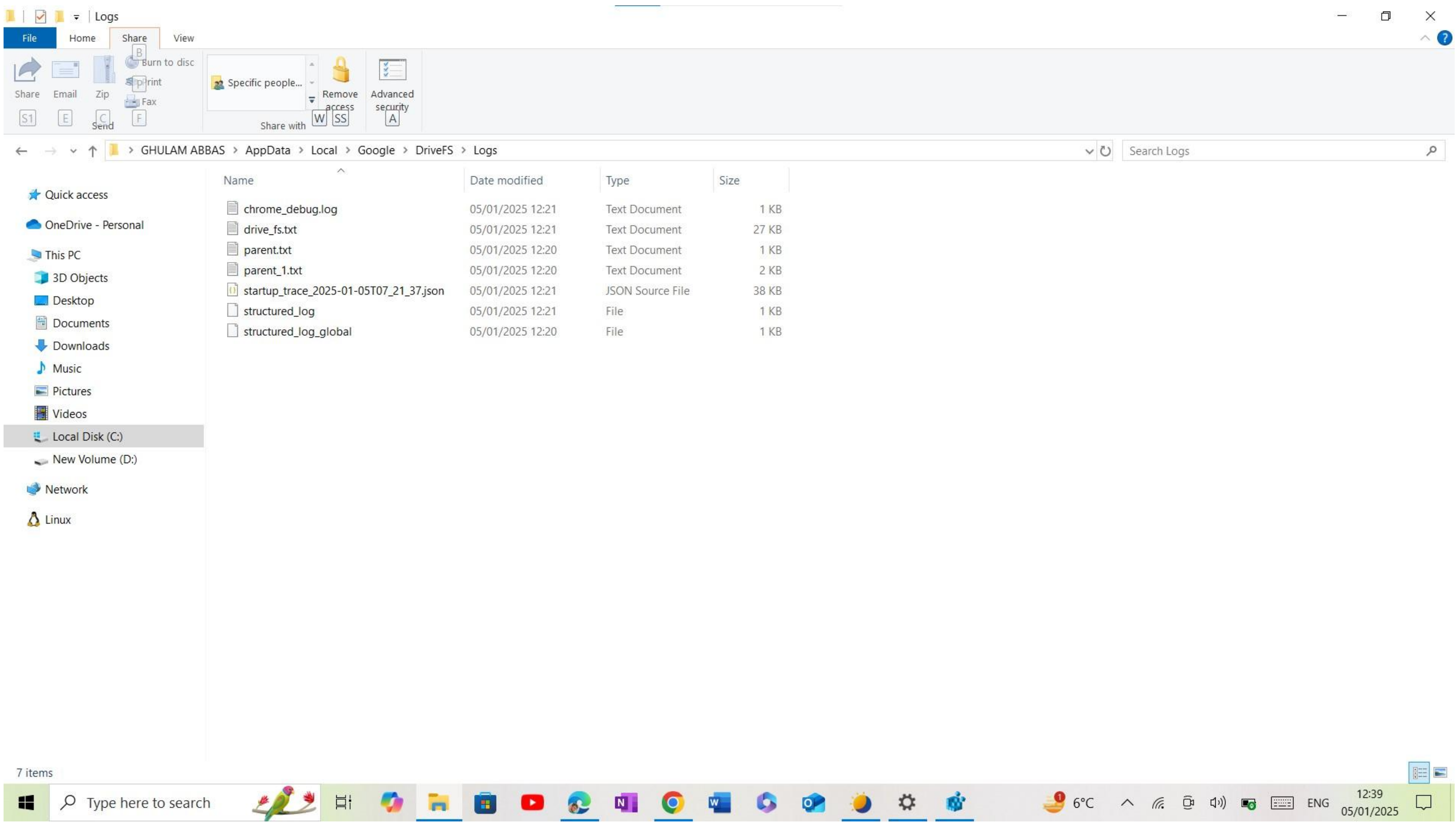
C:\Program Files\Google\Drive File Stream

7 items

III. Configuration Files

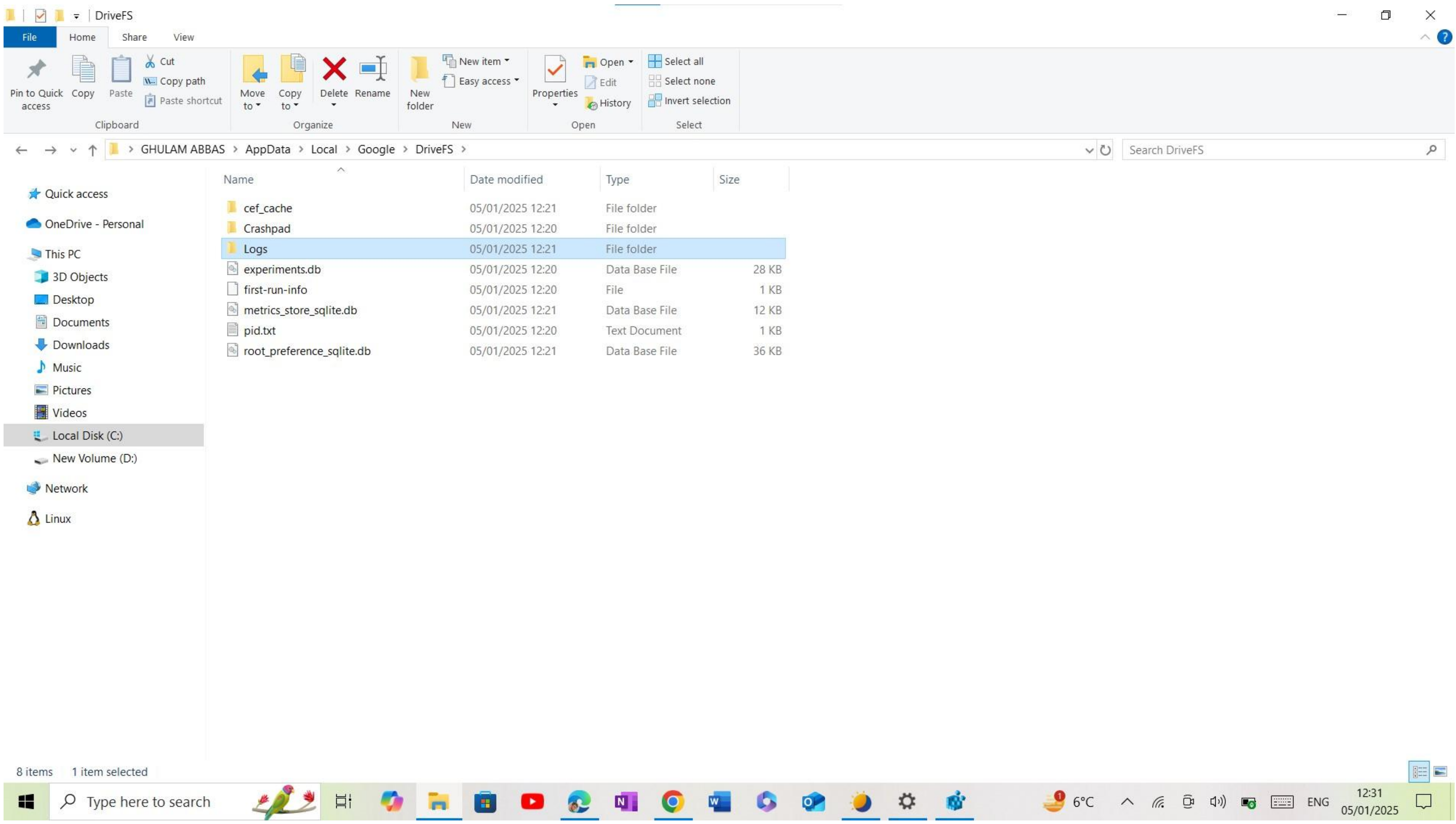
- **Created in user directories:**
  C:\Users\DELL\AppData\Local\Google\DriveFS\Logs

i. Log Files



Name	Date modified	Type	Size
chrome_debug.log	05/01/2025 12:21	Text Document	1 KB
drive_fs.txt	05/01/2025 12:21	Text Document	27 KB
parent.txt	05/01/2025 12:20	Text Document	1 KB
parent_1.txt	05/01/2025 12:20	Text Document	2 KB
startup_trace_2025-01-05T07_21_37.json	05/01/2025 12:21	JSON Source File	38 KB
structured_log	05/01/2025 12:21	File	1 KB
structured_log_global	05/01/2025 12:20	File	1 KB

ii. Configuration Files



GHULAM ABBAS > AppData > Local > Google > DriveFS >

Name	Date modified	Type	Size
cef_cache	05/01/2025 12:21	File folder	
Crashpad	05/01/2025 12:20	File folder	
Logs	05/01/2025 12:21	File folder	
experiments.db	05/01/2025 12:20	Data Base File	28 KB
first-run-info	05/01/2025 12:20	File	1 KB
metrics_store_sqlite.db	05/01/2025 12:21	Data Base File	12 KB
pid.txt	05/01/2025 12:20	Text Document	1 KB
root_preference_sqlite.db	05/01/2025 12:21	Data Base File	36 KB

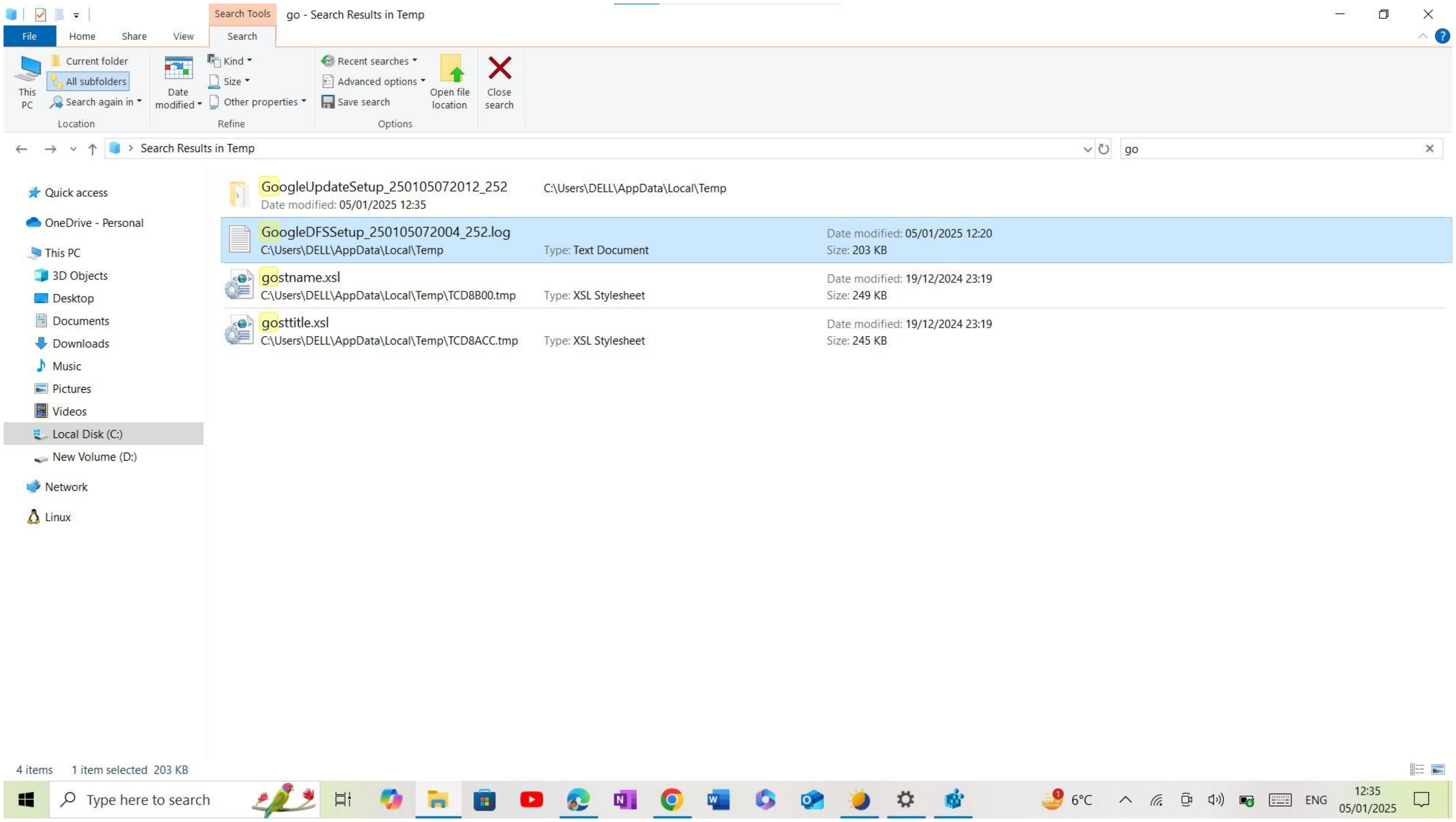
8 items 1 item selected

2. Artifacts created when a file is uploaded or downloaded

i. Temporary Files:

Created during uploads/downloads in:

C:\Users\<username>\AppData\Local\Temp



GoogleUpdateSetup_250105072012_252
Date modified: 05/01/2025 12:35
C:\Users\DELL\AppData\Local\Temp

GoogleDFSSetup_250105072004_252.log
C:\Users\DELL\AppData\Local\Temp
Type: Text Document
Date modified: 05/01/2025 12:20
Size: 203 KB

gostname.xsl
C:\Users\DELL\AppData\Local\Temp\TCD8B00.tmp
Type: XSL Stylesheet
Date modified: 19/12/2024 23:19
Size: 249 KB

gosttitle.xsl
C:\Users\DELL\AppData\Local\Temp\TCD8ACC.tmp
Type: XSL Stylesheet
Date modified: 19/12/2024 23:19
Size: 245 KB

4 items 1 item selected 203 KB

ii. Prefetch File

- **Windows Prefetch Files:**
  Trace of executed processes like **drive.exe**
  Path: **C:\Windows\Prefetch**
- **Purpose of Prefetch Files:**
  Prefetch files are used by Windows to speed up the loading of frequently used applications and files.

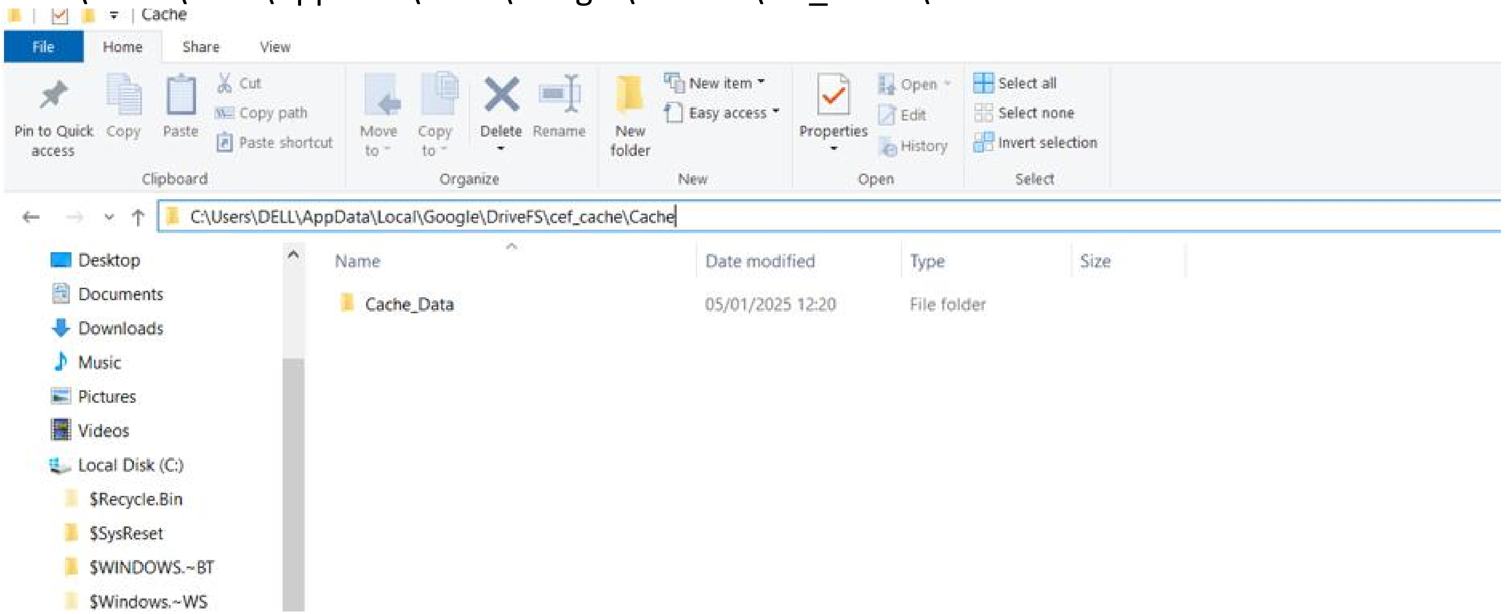
  These files store information about the execution of programs, including their locations and related resource access patterns.
- **File Naming Convention:**
  Prefetch files have names based on the executable they track, followed by a hash value and the `.pf` extension.

  e.g: GoogleDriveFS.pf

iii. Cache

- Google Drive maintains its **own cache directory**, but this is unrelated to the Windows Prefetch system.

  The cache directory is typically found at:
  C:\Users\DELL\AppData\Local\Google\DriveFS\cef_cache\



C:\Users\DELL\AppData\Local\Google\DriveFS\cef_cache\Cache

Name	Date modified	Type	Size
Cache_Data	05/01/2025 12:20	File folder	

3. Logs recorded and their accuracy

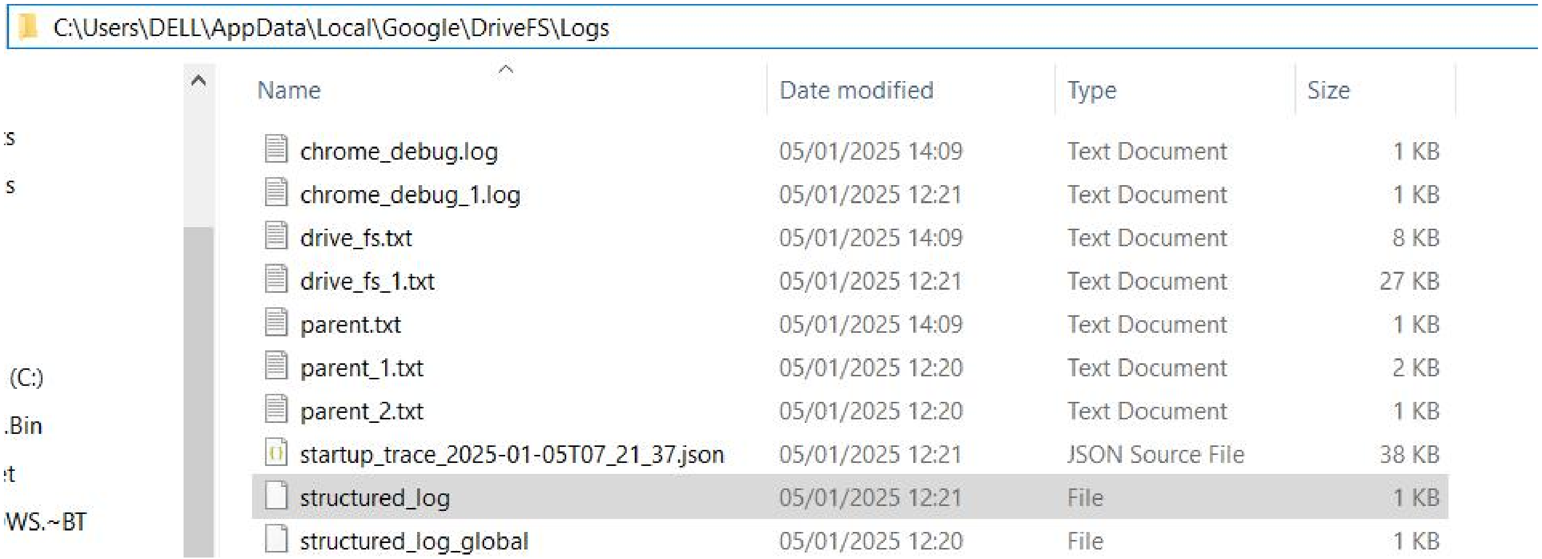
The logs folder for **Google Drive for Desktop** contains various log files that track the application's activities, synchronization events and errors.

C:\Users\DELL\AppData\Local\Google\DriveFS\logs

1. drivefs.log: The primary log file that records detailed information about Google Drive operations.
2. drivefs_events.log: High-level event log summarizing specific actions performed by the application.
3. error.log: Tracks errors encountered by Google Drive during operation.
4. sync_config.db.log: Logs changes to the sync_config.db database file, which tracks the configuration and sync states.

Accuracy: -

- Google Drive sync logs are highly accurate and reliable for forensic investigations, especially when combined with other system artifacts.
- Proper validation techniques (e.g., hashing, cross-referencing with metadata) enhance their evidentiary value.



Name	Date modified	Type	Size
chrome_debug.log	05/01/2025 14:09	Text Document	1 KB
chrome_debug_1.log	05/01/2025 12:21	Text Document	1 KB
drive_fs.txt	05/01/2025 14:09	Text Document	8 KB
drive_fs_1.txt	05/01/2025 12:21	Text Document	27 KB
parent.txt	05/01/2025 14:09	Text Document	1 KB
parent_1.txt	05/01/2025 12:20	Text Document	2 KB
parent_2.txt	05/01/2025 12:20	Text Document	1 KB
startup_trace_2025-01-05T07_21_37.json	05/01/2025 12:21	JSON Source File	38 KB
structured_log	05/01/2025 12:21	File	1 KB
structured_log_global	05/01/2025 12:20	File	1 KB

4. Artifact left behind after uninstallation

- **Residual Files:**

Unremoved directories:

`C:\Users\DELL\AppData\Local\Google\Drive\`

Leftover files include `log`, `cache`, or `temp` data.

- **Registry Keys:**

Orphaned keys in `HKCU` or `HKLM` related to Google Drive.

- **Windows Event Logs:**

Entries showing uninstallation events

Step 1. Open File Explorer.

Navigate to the directory:

C:\Users\<username>\AppData\Local\Google\DriveFS\logs

Step 2: Identify Relevant Log Files

Focus on the following log files that might contain uninstallation events:

`drivefs.log` (main activity log).

`drivefs_events.log` (high-level events log).

`error.log` (captures errors, including uninstallation-related errors).

Step 3: Open the Logs

Open the log files using:

Notepad (basic viewing).

Notepad++ or any log viewer tool for better readability and searching capabilities.

Ensure you enable **word wrap** or use a log viewer tool that supports large files for efficient navigation.

Step 4: Search for Uninstallation Events

Use keywords or phrases commonly associated with uninstallation:

Keywords to Search:

```
UNINSTALL
DELETED
DRIVEFS STOPPED
SERVICE REMOVED
Uninstallation complete
```

5. other resources of Information

I. Cross-Check Browsers artifacts

For chrome: C:\Users\DELL\AppData\Local\Google\Chrome\User Data\Default

For Edge: C:\Users\DELL\AppData\Local\Microsoft\Edge\User Data\Default

Analyze the cookies, saved sessions and cached files of recently accessed documents.

II. Capture Network Traffic

Use a packet capture tool like **Wireshark** (if live monitoring was set up during uninstallation).

Filter network traffic

Destination: google.com or googleusercontent.com.

Protocols use: HTTP/HTTPS

Network activity during uninstallation.

Requests for removing or syncing files with the cloud.

III. Examine Email records

Check the user's email account for:

Notifications of file sharing.

Alerts related to account or app changes.

Search email clients like:

Outlook: Default PST/OST file location:
C:\Users\DELL\AppData\Local\Microsoft\Outlook

Gmail: Search Google Takeout for email data exports.

6. Artifacts left behind when files shared

System-Level Artifacts (Local Machine)

1. Logs

C:\Users\<username>\AppData\Local\Google\DriveFS\logs

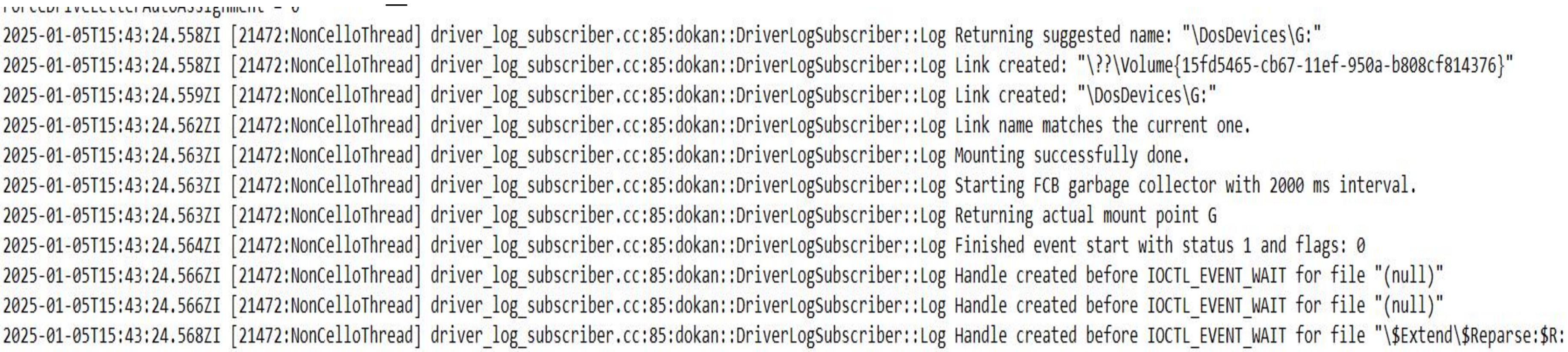
- Relevant Logs:

`drivefs.log`
`drivefs_events.log`

- What to Look For:

Search for keywords like:

`SHARED`
`LINK_CREATED`
`PERMISSION_UPDATED`



```
ForceDriveLetterAutoAssignment = 0
2025-01-05T15:43:24.558ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Returning suggested name: "\DosDevices\G:"
2025-01-05T15:43:24.558ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Link created: "\??\Volume{15fd5465-cb67-11ef-950a-b808cf814376}"
2025-01-05T15:43:24.559ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Link created: "\DosDevices\G:"
2025-01-05T15:43:24.562ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Link name matches the current one.
2025-01-05T15:43:24.563ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Mounting successfully done.
2025-01-05T15:43:24.563ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Starting FCB garbage collector with 2000 ms interval.
2025-01-05T15:43:24.563ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Returning actual mount point G
2025-01-05T15:43:24.564ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Finished event start with status 1 and flags: 0
2025-01-05T15:43:24.566ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Handle created before IOCTL_EVENT_WAIT for file "(null)"
2025-01-05T15:43:24.566ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Handle created before IOCTL_EVENT_WAIT for file "(null)"
2025-01-05T15:43:24.568ZI [21472:NonCelloThread] driver_log_subscriber.cc:85:dokan::DriverLogSubscriber::Log Handle created before IOCTL_EVENT_WAIT for file "\$Extend\$Reparse:$R:
```

2. Database Files

C:\Users\<username>\AppData\Local\Google\DriveFS\user_default

- Relevant Files:

`sync_config.db`
`metrics_store_sqlite.db`

- What to Look For:

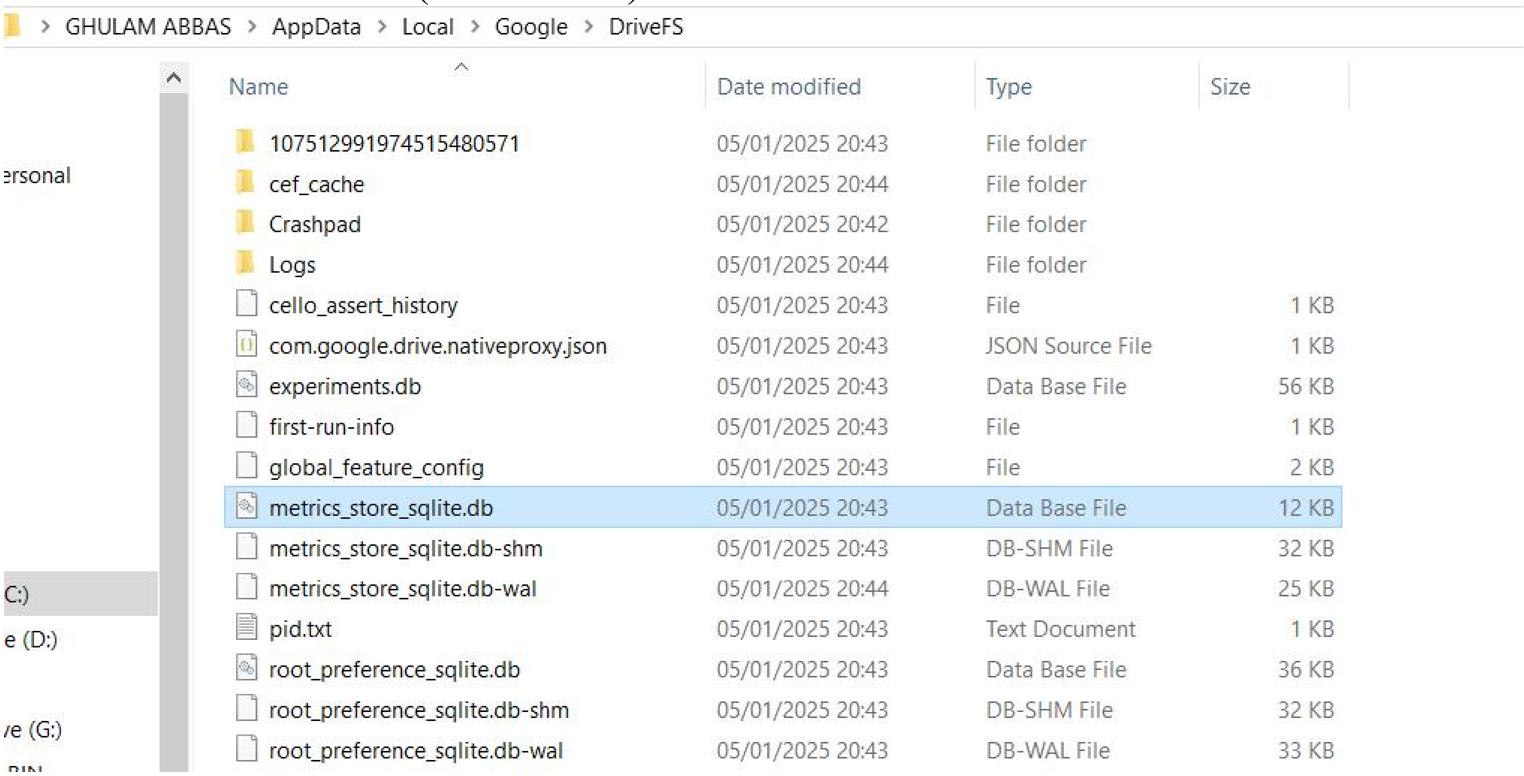
Analyze these databases using tools like SQLite Browser.

Check for:

File IDs

Sharing timestamps

User email addresses (shared with)



GHULAM ABBAS > AppData > Local > Google > DriveFS

Name	Date modified	Type	Size
107512991974515480571	05/01/2025 20:43	File folder	
cef_cache	05/01/2025 20:44	File folder	
Crashpad	05/01/2025 20:42	File folder	
Logs	05/01/2025 20:44	File folder	
cello_assert_history	05/01/2025 20:43	File	1 KB
com.google.drive.nativeproxy.json	05/01/2025 20:43	JSON Source File	1 KB
experiments.db	05/01/2025 20:43	Data Base File	56 KB
first-run-info	05/01/2025 20:43	File	1 KB
global_feature_config	05/01/2025 20:43	File	2 KB
metrics_store_sqlite.db	05/01/2025 20:43	Data Base File	12 KB
metrics_store_sqlite.db-shm	05/01/2025 20:43	DB-SHM File	32 KB
metrics_store_sqlite.db-wal	05/01/2025 20:44	DB-WAL File	25 KB
pid.txt	05/01/2025 20:43	Text Document	1 KB
root_preference_sqlite.db	05/01/2025 20:43	Data Base File	36 KB
root_preference_sqlite.db-shm	05/01/2025 20:43	DB-SHM File	32 KB
root_preference_sqlite.db-wal	05/01/2025 20:43	DB-WAL File	33 KB

7. *Information present in the database files*

Path to Database Files

The database files for Google Drive are typically located at:

C:\Users\<username>\AppData\Local\Google\DriveFS\user_default

Key Database Files

Tools: SQLite viewer

1. sync_config.db

Contains information about files being synced.

Tracks local-to-cloud mappings (file paths, IDs, sync status).

2. metrics_store_sqlite.db

Stores metrics such as user activity, app performance, and sync event timestamps.

C:\Users\<username>\AppData\Local\Google\DriveFS\user_default\metrics_store_sqlite.db

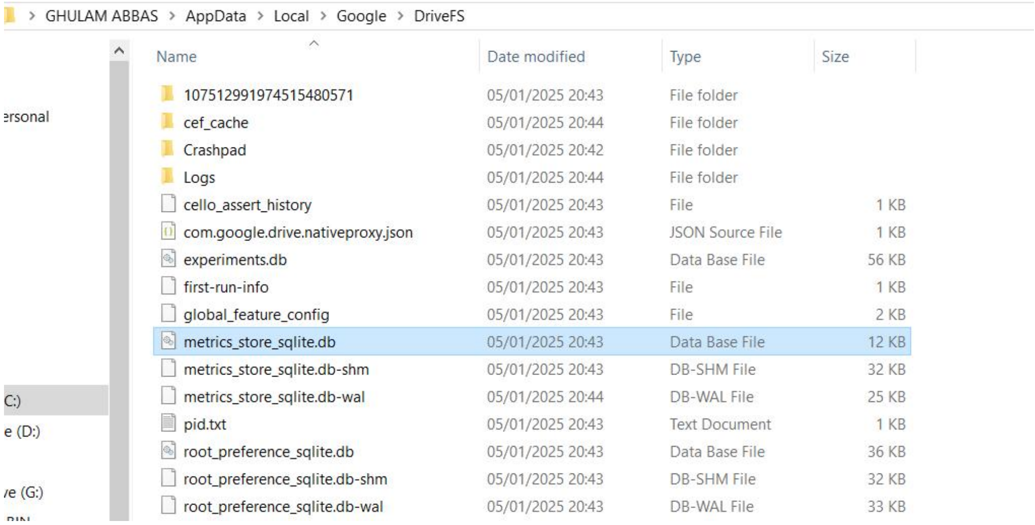
3. root_preference_sqlite.db

Contains user preferences and configuration settings for Google Drive.

C:\Users\<username>\AppData\Local\Google\DriveFS\user_default\metrics_store_sqlite.db

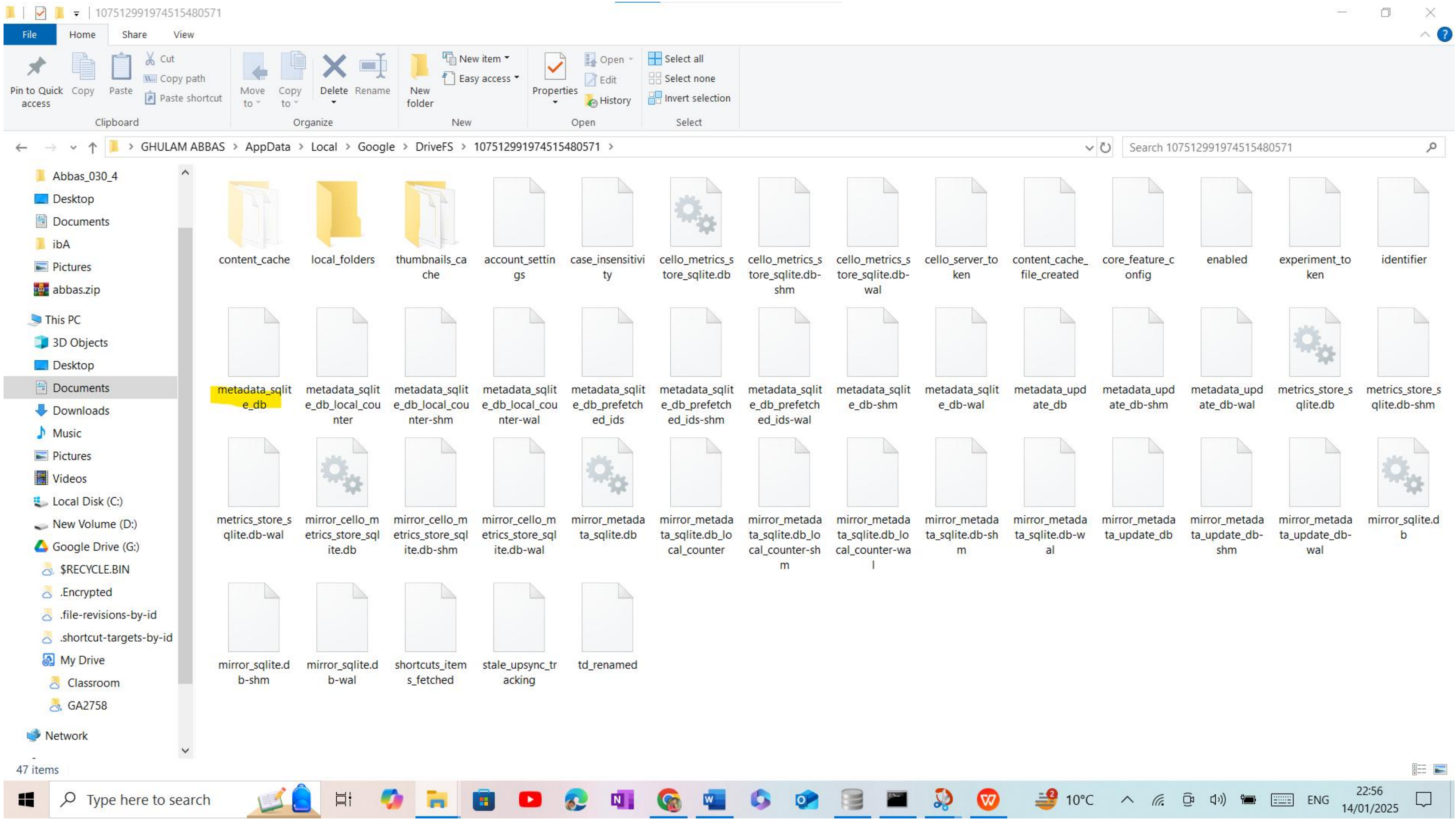
Mirror_Metedata_sqlite.db

Show all files that are upload on google drive



Name	Date modified	Type	Size
107512991974515480571	05/01/2025 20:43	File folder	
cef_cache	05/01/2025 20:44	File folder	
Crashpad	05/01/2025 20:42	File folder	
Logs	05/01/2025 20:44	File folder	
cello_assert_history	05/01/2025 20:43	File	1 KB
com.google.drive.nativeproxy.json	05/01/2025 20:43	JSON Source File	1 KB
experiments.db	05/01/2025 20:43	Data Base File	56 KB
first-run-info	05/01/2025 20:43	File	1 KB
global_feature_config	05/01/2025 20:43	File	2 KB
metrics_store_sqlite.db	05/01/2025 20:43	Data Base File	12 KB
metrics_store_sqlite.db-shm	05/01/2025 20:43	DB-SHM File	32 KB
metrics_store_sqlite.db-wal	05/01/2025 20:44	DB-WAL File	25 KB
pid.txt	05/01/2025 20:43	Text Document	1 KB
root_preference_sqlite.db	05/01/2025 20:43	Data Base File	36 KB
root_preference_sqlite.db-shm	05/01/2025 20:43	DB-SHM File	32 KB
root_preference_sqlite.db-wal	05/01/2025 20:43	DB-WAL File	33 KB

Shows All .db files of Google drive



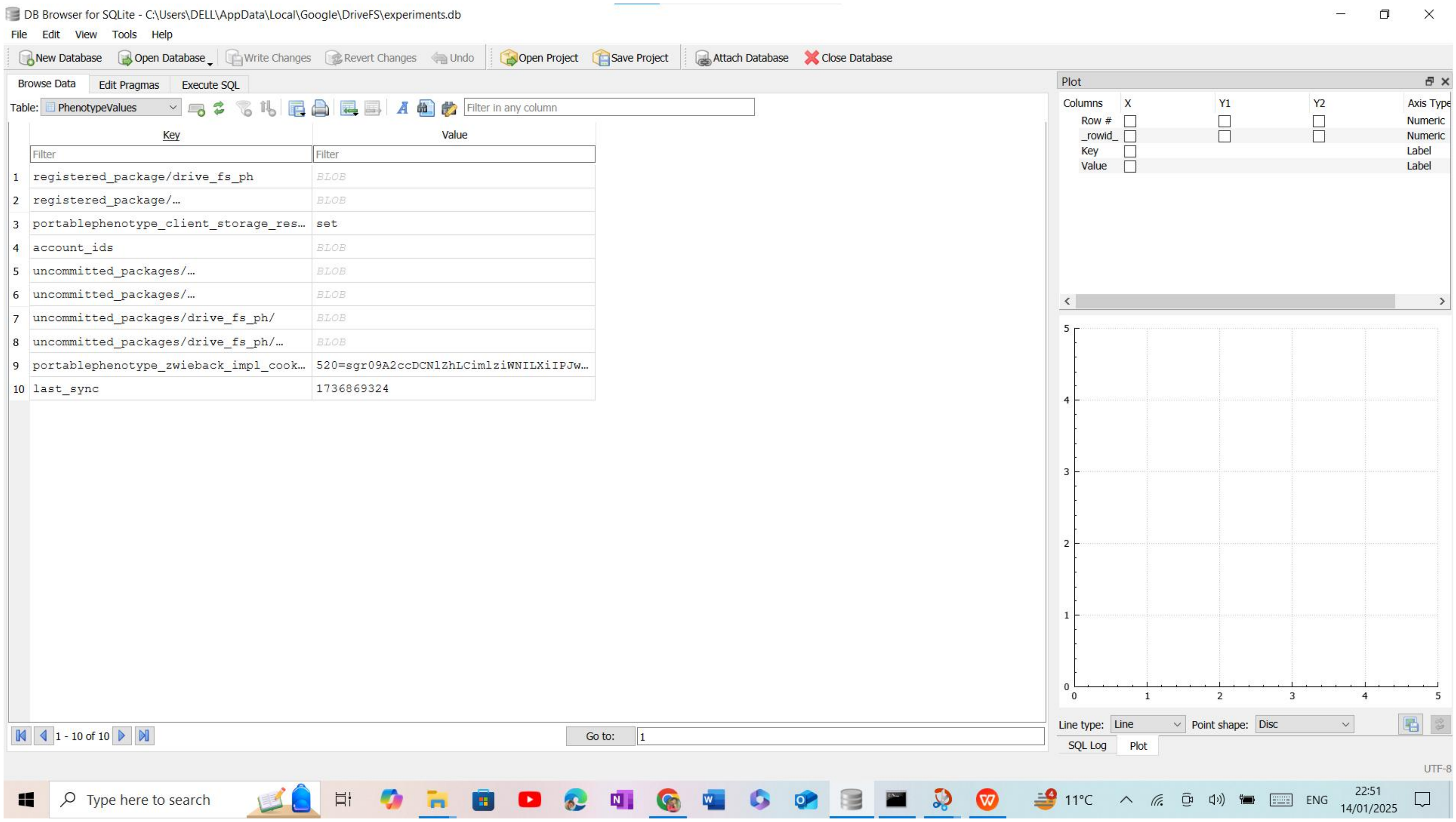
GHULAM ABBAS > AppData > Local > Google > DriveFS > 107512991974515480571 >

content_cache
local_folders
thumbnails_cache
account_settings
case_insensitivity
cello_metrics_store_sqlite.db
cello_metrics_store_sqlite.db-shm
cello_metrics_store_sqlite.db-wal
cello_server_token
content_cache_file_created
core_feature_config
enabled
experiment_token
identifier
metadata_sqlite_db
metadata_sqlite_db_local_counter
metadata_sqlite_db_local_counter-shm
metadata_sqlite_db_local_counter-wal
metadata_sqlite_db_prefetched_ids
metadata_sqlite_db_prefetched_ids-shm
metadata_sqlite_db_prefetched_ids-wal
metadata_sqlite_db-shm
metadata_sqlite_db-wal
metadata_update_db
metadata_update_db-shm
metadata_update_db-wal
metrics_store_sqlite.db
metrics_store_sqlite.db-shm
metrics_store_sqlite.db-wal
mirror_cello_metrics_store_sqlite.db
mirror_cello_metrics_store_sqlite.db-shm
mirror_cello_metrics_store_sqlite.db-wal
mirror_metadata_sqlite.db
mirror_metadata_sqlite.db_local_counter
mirror_metadata_sqlite.db_local_counter-shm
mirror_metadata_sqlite.db_local_counter-wal
mirror_metadata_sqlite.db-shm
mirror_metadata_sqlite.db-wal
mirror_metadata_update_db
mirror_metadata_update_db-shm
mirror_metadata_update_db-wal
mirror_sqlite.db
mirror_sqlite.db-shm
mirror_sqlite.db-wal
shortcuts_items_fetched
stale_upsync_tracking
td_renamed

47 items

Key Insights from the experiments.db Screenshot

1. **Registered Packages:**
   - **Key:** `registered_package/drive_fs_ph` and similar entries.
   - **Value:** Likely contains information about packages or modules related to Google Drive features that are registered for the user or system. These might be in BLOB (binary large object) format.



DB Browser for SQLite - C:\Users\DELL\AppData\Local\Google\DriveFS\experiments.db

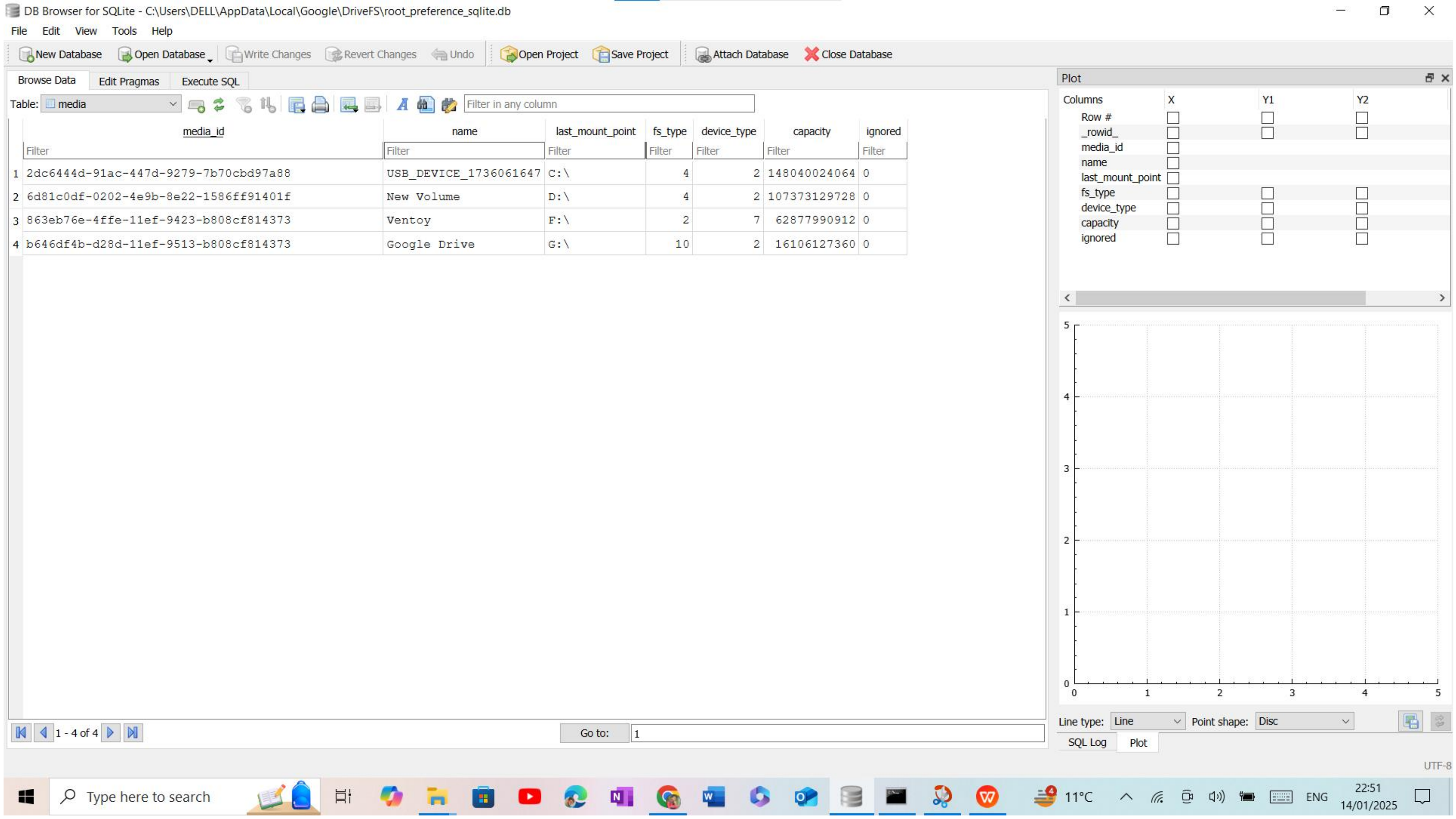
Table: PhenotypeValues

	Key	Value
1	registered_package/drive_fs_ph	BLOB
2	registered_package/…	BLOB
3	portablephenotype_client_storage_res…	set
4	account_ids	BLOB
5	uncommitted_packages/…	BLOB
6	uncommitted_packages/…	BLOB
7	uncommitted_packages/drive_fs_ph/	BLOB
8	uncommitted_packages/drive_fs_ph/…	BLOB
9	portablephenotype_zwieback_impl_cook…	520=sgr09A2ccDCNlZhLCimlziWNILXiIPJw…
10	last_sync	1736869324

1 - 10 of 10

22:51
14/01/2025

The screenshot displays the `root_preference_sqlite.db` database, which stores information about connected media and devices associated with Google Drive.



DB Browser for SQLite - C:\Users\DELL\AppData\Local\Google\DriveFS\root_preference_sqlite.db

Table: media

	media_id	name	last_mount_point	fs_type	device_type	capacity	ignored
1	2dc6444d-91ac-447d-9279-7b70cbd97a88	USB_DEVICE_1736061647	C:\	4	2	148040024064	0
2	6d81c0df-0202-4e9b-8e22-1586ff91401f	New Volume	D:\	4	2	107373129728	0
3	863eb76e-4ffe-11ef-9423-b808cf814373	Ventoy	F:\	2	7	62877990912	0
4	b646df4b-d28d-11ef-9513-b808cf814373	Google Drive	G:\	10	2	16106127360	0

1 - 4 of 4

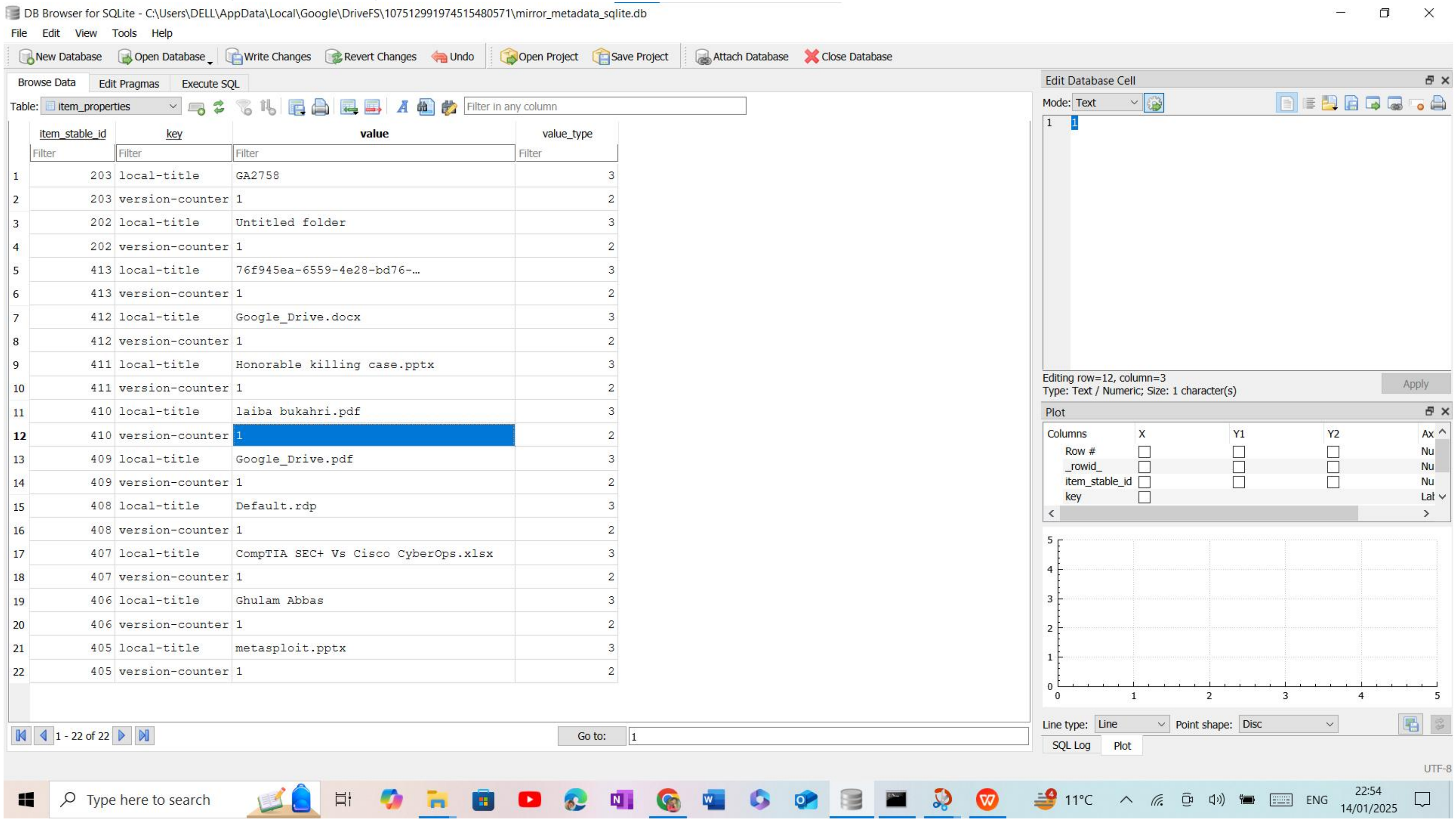
Go to: 1

Columns	X	Y1	Y2
Row #	□	□	□
rowid	□	□	□
media_id	□		
name	□		
last_mount_point	□		
fs_type	□	□	□
device_type	□	□	□
capacity	□	□	□
ignored	□	□	□

Line type: Line

Point shape: Disc

These are files that uploaded in my drive



DB Browser for SQLite - C:\Users\DELL\AppData\Local\Google\DriveFS\107512991974515480571\mirror_metadata_sqlite.db

Table: item_properties

	item_stable_id	key	value	value_type
1	203	local-title	GA2758	3
2	203	version-counter	1	2
3	202	local-title	Untitled folder	3
4	202	version-counter	1	2
5	413	local-title	76f945ea-6559-4e28-bd76-…	3
6	413	version-counter	1	2
7	412	local-title	Google_Drive.docx	3
8	412	version-counter	1	2
9	411	local-title	Honorable killing case.pptx	3
10	411	version-counter	1	2
11	410	local-title	laiba bukahri.pdf	3
12	410	version-counter	1	2
13	409	local-title	Google_Drive.pdf	3
14	409	version-counter	1	2
15	408	local-title	Default.rdp	3
16	408	version-counter	1	2
17	407	local-title	CompTIA SEC+ Vs Cisco CyberOps.xlsx	3
18	407	version-counter	1	2
19	406	local-title	Ghulam Abbas	3
20	406	version-counter	1	2
21	405	local-title	metasploit.pptx	3
22	405	version-counter	1	2

1 - 22 of 22

Editing row=12, column=3
Type: Text / Numeric; Size: 1 character(s)

All screenshots showing the artifact of google drive. User download google drive on system and upload multiple files on the google drive

8. Artifacts left after using anti-forensics tool

1. Examine Disk Artifacts

Deleted files may leave behind:

File fragments in unallocated disk space.

File system metadata (e.g., MFT entries in NTFS).

Steps to Recover Fragments:

Use a forensic disk imaging tool like FTK Imager**:**

Create a forensic copy of the disk.

Scan for residual data in unallocated space.

Analyze with recovery tools like Autopsy**:**

Look for fragments related to Google Drive directories or file names.

What to Look For:

Deleted file fragments with recognizable content.

Timestamps and partial filenames.

2. **Examine Event Logs**

Windows Event Logs

Attempts to disable synchronization, clear data, or uninstall Google Drive may leave traces in:

Security Logs: Tracks file access and modification.

Application Logs: Records app crashes or errors.

Setup Logs: Tracks uninstallation events.

Path to Event Viewer:

Open **Event Viewer**:

Control Panel > Administrative Tools > Event Viewer

Navigate to:

Windows Logs > Security

Applications and Services Logs

Look For:

Keywords: DriveFS, FileStream, Delete, Sync.

3. Investigate Metadata Remnants

Partial Metadata in Database Files

Even if files are deleted using anti-forensics tools, **database records** may still contain:

File IDs.

Names or paths of deleted files.

Sync timestamps.

Logs of previous sync activity.

Steps to Extract Metadata:

Open the relevant database file:

Path:

C:\Users\<username>\AppData\Local\Google\DriveFS\user_default\sync_config.db

Use a tool like **DB Browser for SQLite**.

Run queries to locate orphaned entries:

```
SELECT * FROM items WHERE status = 'deleted';
```

Look for **timestamps** of deletion events or residual records that may not have been purged by the tool.