International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 12 | Dec 2025 www.irjet.net p-ISSN: 2395-0072

Digital Forensic Analysis of Google Drive Activities in Windows Systems

Dija S, Veena Vijayan

Centre for Development of Advanced Computing, Thiruvanathapuram, India

---

Abstract - *Browser Forensics is an inevitable part in a cyber-crime investigations due to the high dependence on internet for everyday tasks. Thus, identifying a suspect's Internet activities and browser habits is crucial in any investigation. In that context, a particularly important aspect is collecting information about files uploaded to and downloaded from cloud-based storage platforms such as Google Drive. Every interaction with Google Drive—whether uploading or downloading—produces a set of artifacts on a Windows OS System. These details appear in locally-generated Browser Files by Web Browsers and logs created by the locally installed Google Drive application. This research presents a novel forensic methodology for identifying Google Drive activities done in a Windows OS System and the associated details including name and email-id of the user, who initiated the activity. It analyzes the browser files stored locally across major web browsers, Chrome, Edge, Opera, Yandex, UC Browser, Maxthon, and Firefox. It also analyzes the log files saved by the local Google Drive application to identify the Google Drive activities. The paper outlines artifact locations along with the forensic significance to correlate and reconstruct crucial Internet activities of the Suspect related to the Google Drive Activities. The results demonstrate how cybercrime investigators can accurately identify a suspect's Google Drive activities in A Windows OS System.*

Key Words: **Digital Forensics, Google Drive Forensics, Browser Forensics, Cloud Forensics, Internet Forensics**

1. INTRODUCTION

Web browsers have become the primary gateway to the Internet in everyday computing, supporting everything from routine browsing to critical business operations, which is why they play a major role in cybercrime investigations. Browser forensics focuses on locating and interpreting the traces created by the Web Browser. This includes crucial information including the details like visited websites, search queries, downloaded files, bookmarks, cookies, and cached content, all of which help investigators understand what a user was doing online. The browsers store a significant amount of this information locally in the form of SQLite databases, JSON files, cache folders, and session data, providing dependable evidence of browsing activities. This data becomes an important source of evidence in digital investigations, especially when trying to link user behavior with the Google Drive Activities.

Cloud services have become deeply embedded in daily computing workflows, enabling rapid data sharing and flexible access from multiple devices. While these features improve productivity, they also create opportunities for misuse by the criminals. Criminals increasingly leverage cloud platforms to store, transfer, and conceal digital evidence or illicit material. Studies on cloud storage forensics emphasize the rising frequency of incidents involving Google Drive misuse in data theft, intellectual property breaches, and various types of cybercrimes [1].

Every action performed through Google Drive generates identifiable local traces in a Windows OS system. This includes authentication through email credentials and upload/download operations. These actions leave behind browser-level artifacts in SQLite databases, cookies, session restore files, JSON metadata, and IndexedDB caches. Prior forensic studies highlight the persistence and evidentiary value of these artifacts [3], [4], [7]. Beyond web browsers, the Google Drive Desktop App—DriveFS—maintains a rich collection of logs, metadata caches, and internal event records. These include file synchronization details, remote FileIDs, local file paths, upload/download timestamps, and account identifiers. DriveFS logs are instrumental for reconstructing timelines that are otherwise incomplete from browser sources alone.

2. BROWSER FORENSICS

Browser forensics is an indispensable component of Google Drive investigations, as most Drive interactions occur through web browsers. Most of the users may not locally install the Google Drive Application their systems. Thus the major focus of the Investigators while trying to analyze Forensic research consistently shows that browsers retain extensive remnants of cloud service usage [3], [4], [7], [9]. These remnants serve as evidence of Gmail accounts used, sessions initiated, and Drive files accessed.

2.1 Browser File Locations

The default locations for browser profile artifacts in commonly used web browsers on a Windows system are listed in Table 1. These artifacts are stored within the "OS_Drive://Users/User/AppData" directory, and depending on the browser, the files may be located either in the "Local" folder or the "Roaming" folder.

Table -1: Key Browser Forensic files with email-ids

Path of Browser Forensic files		
Sl. No	Web Browser	File Path
1	Google Chrome	...\Local\Google\Chrome\User Data\Default\
2	Microsoft Edge	...\Local\Microsoft\Edge\User Data\Default\
3	Opera	...\Roaming\Opera Software\Opera Stable\
4	Yandex Browser	...\Local\Yandex\YandexBrowser\User Data\Default\
5	UC Browser	...\Local\UCBrowser\User Data\
6	Maxthon	...\Roaming\ Maxthon3\User Data\<Profile>\
7	Mozilla Firefox	...\Roaming\Mozilla\Firefox\Profiles\<RANDOM>.default\

2.2 Browsers-by-Browser Artifact Analysis

Chromum based browsers are a rich source of Drive artifacts due to stable SQLite schemas and IndexedDB architecture [4], [5], [7]. Artifacts include: Google Chrome hold the following details.

- Visit history (Drive folder/file URLs containing FileIDs).
- Cookies storing Gmail session and Drive authentication tokens.
- Auto fills Gmail IDs.
- Saved login records.
- Cached Drive web app metadata stored in IndexedDB.

Microsoft Edge mirrors Chrome but stores persistent cookies longer due to partitioned storage and telemetry integrations [3]. Yandex Browser often stores long-lived login tokens and Google cookies [9]. UC Browser uses legacy storage structures, storing Gmail IDs and Drive metadata even when Chrome is wiped [3]. Maxthon's mixed architecture leads to retention of both WebKit and Chromium artifacts [7]. Mozilla Firefox: Firefox stores Drive interactions in:

- places.sqlite (history)
- cookies.sqlite (Gmail authentication)
- formhistory.sqlite (Gmail IDs)
- logins.json (saved credentials)
- sessionstore.jsonlz4 (open Drive tabs)

2.3 Identification of Google Drive artifacts from Browser generated Files

From the research conducted with the various artifacts available in the browser files generated in a Windows OS system, the following are the information related to Google Drive artifacts found.

- History: Reveals Drive folder browsing and file previews.
- Cookies: Associates actions with specific Gmail logins.
- Autofill: Shows Gmail IDs ever typed.
- Login Data: Shows saved or attempted identities.

These artifacts are central to reconstructing user intended activities in the Google Drive [3], [9], [11].

Table -2: Key Browser Forensic files holding email-ids

Key Browser Forensic files with email-ids				
Sl. No	Web Browser	File Name	Artifacts	Format
1	Google Chrome/ Microsoft Edge/ Opera/ Yandex Browser/ Maxthon Browser	Web Data	Autofill Mail IDs	SQLite
2		Login Data	Mail IDs / usernames	SQLite
3	UC Browser	Web Data	Gmail form-fill entries	SQLite
		IndexedB	Mail Ids	LevelDB
4	Mozilla Firefox	formhistory.sqlite	Autofill Gmail IDs	SQLite

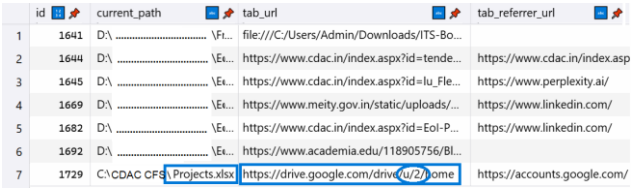
Tables 2 and 3 present the key browser artifact files that store information related to Google Drive activities on a Windows OS System. Table 2 lists the primary artifacts that contain user email IDs extracted from commonly used web browsers. In contrast, Table 3 outlines the artifact files from which Drive-related URLs and file details can be retrieved.

Table -3: Key Browser Forensic files holding Google Drive Artifacts

Key Browser Forensic files in Google Drive Artifacts – Drive URL & File Name				
Sl. No	Web Browser	File Name	Artifacts	Format
1	Google Chrome /Microsoft Edge /Opera /Yandex Browser /UC Browser /Maxthon Browser	History	Drive URLs, File Details, downloads	SQLite
2	Mozilla Firefox	places.sqlite	Drive URLs, file preview/download events	SQLite

From the detailed case studies conducted with Google Chrome web browser, it has been identified that the browser files reveal the Drive URL visited, the file that was uploaded or downloaded, and the email address associated with that activity. The following section describes the extraction steps in detail. First, a Google Drive visit can be confirmed by locating the Drive URL in Chrome's locally stored history. Fig. 1 shows a URL entry recovered from the downloads table in the History SQLite database.

After the Drive visit is verified, the next step is to identify the specific file that was accessed. Fig. 1 displays the file name along with the folder path of the accessed file. The final and most important step is to identify the details of the user. For this, the Drive URL is to be parsed to extract the profile identifier (the /u/n/ segment), then identify the associated profile details stored in another browser file to recover the user's email and profile information. The following sections explain each of these steps and the supporting artifacts in greater detail.



	id	current_path	tab_url	tab_referrer_url
1	1641	D:\ ..... \Fr...	file:///C:/Users/Admin/Downloads/ITS-Bo...	
2	1644	D:\ ..... \Ex...	https://www.cdac.in/index.aspx?id=tende...	https://www.cdac.in/index.asp
3	1645	D:\ ..... \Ex...	https://www.cdac.in/index.aspx?id=lu_Fle...	https://www.perplexity.ai/
4	1669	D:\ ..... \Ex...	https://www.meity.gov.in/static/uploads/...	https://www.linkedin.com/
5	1682	D:\ ..... \Ex...	https://www.cdac.in/index.aspx?id=EoI-P...	https://www.linkedin.com/
6	1692	D:\ ..... \Ex...	https://www.academia.edu/118905756/Bl...	
7	1729	C:\CDAC CFS\Projects.xlsx	https://drive.google.com/drive/u/2/home	https://accounts.google.com/

Fig -1: File Name and URLs found in Browser Files

The accessed URL recovered is, that is shown in Fig 1 is, https://drive.google.com/drive/u/2/home Sometime, it can be https://drive.google.com/drive/u/1/home Or https://drive.google.com/drive/u/0/home depending on the email-id of the user who accesses the Google Drive.

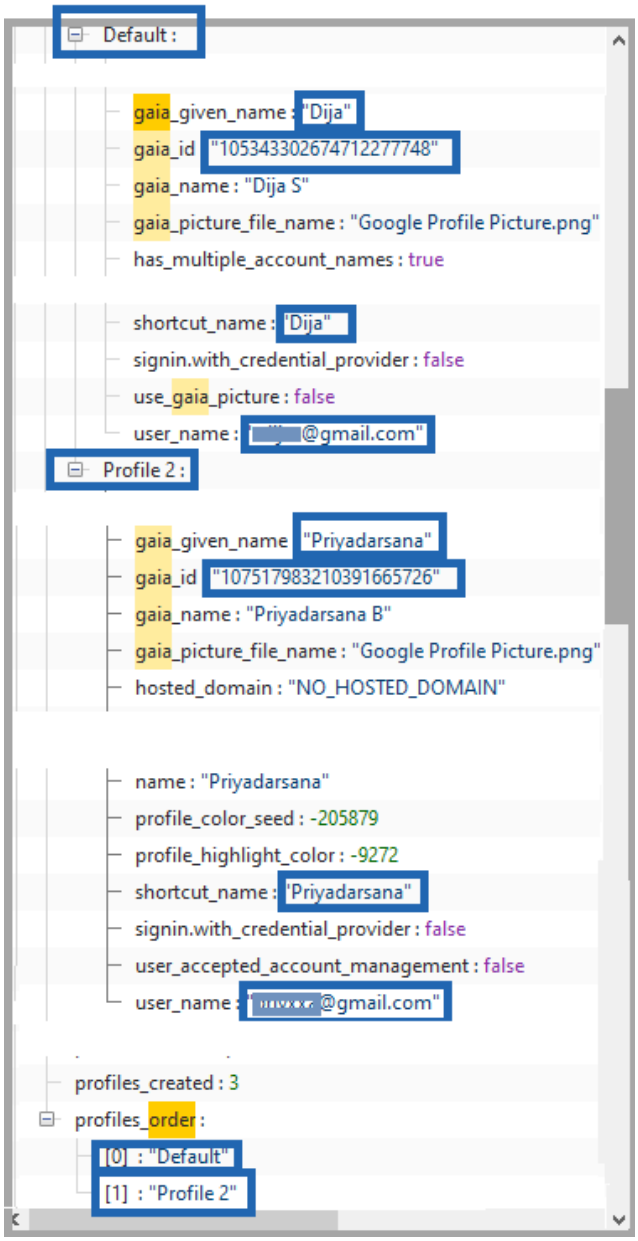


Fig -2: The details of multiple profiles in Google Chrome web browser.

The substring in the Google Drive URL—such as "/u/0/", "/u/1/", or "/u/2/"—indicates which user profile accessed the Drive content. Additional details about these users can be found in the "Local State" file, a JSON-formatted configuration file generated by Google Chrome. Within this file, the "profile" → "info-cache" section lists information for the Default profile as well as any additional profiles, as illustrated in Fig. 2. This includes the user's email ID, name, and other associated details. The file also contains the "profiles_order" entry under the "profile" header, which specifies the profile numbers and corresponding folder names. By referencing this information, investigators can

accurately interpret the "/u/n/" identifiers in the URL and determine which user profile performed the Google Drive activity.

In Fig. 2, two profiles are listed: the Default profile and Profile 2. The Default profile is assigned the number '0', while Profile 2 is assigned the number '2'. Our analysis of multiple Google Drive activities shows that the Default user always accesses Drive using the URL pattern https://drive.google.com/drive/u/0/home, whereas Profile 2 uses https://drive.google.com/drive/u/2/home. Therefore, in Fig. 1, the file "C:\CDAC CFS\Projects.xlsx" was accessed by the Profile 2 user, whose email ID can be identified from the "Local State" JSON file shown earlier. Using this approach, investigators can accurately determine which email account accessed specific Google Drive files. The "Local State" file also stores additional user attributes, including the GAIA ID. GAIA (Google Accounts and ID Administration) is Google's internal identity management system used to create and maintain Google account identities. Importantly, the same GAIA ID appears consistently for a given email ID across both Chrome browser artifacts and DriveFS logs—where it is referred to as the persistable_token. By correlating these identifiers across sources, investigators can reliably attribute Google Drive activities to specific user accounts. This three-step procedure enables a complete reconstruction of user actions from locally generated browser and DriveFS artifacts, providing valuable forensic evidence in cybercrime investigations.

2.4 GOOGLE DRIVE DESKTOP APP (DriveFS) Artifacts

The local files generated by the Google Drive Desktop App (DriveFS) are stored in the path Local\Google\DriveFS within the OS_Drive://Users/User/AppData directory on a Windows system. DriveFS generates several critical forensic artifacts:

- sync_journal.db
- metadata_cache.sqlite
- sync_log.log
- JSON configuration files
- Account-linked folders under DriveFS directories

These artifacts contain details such as uploaded and downloaded files, associated Gmail account identifiers, and local file paths—all of which are highly valuable in a cybercrime investigation.

2.5 Identification of Google Drive artifacts from DriveFS generated Files

In the artifacts generated by DriveFS, the GAIA ID—Google's 64-bit unique identifier for each user—also plays a key role. Within DriveFS, this identifier appears as the persistable_token. The following sections explain how this value can be used to identify and separate the activities of each email account associated with the DriveFS application.

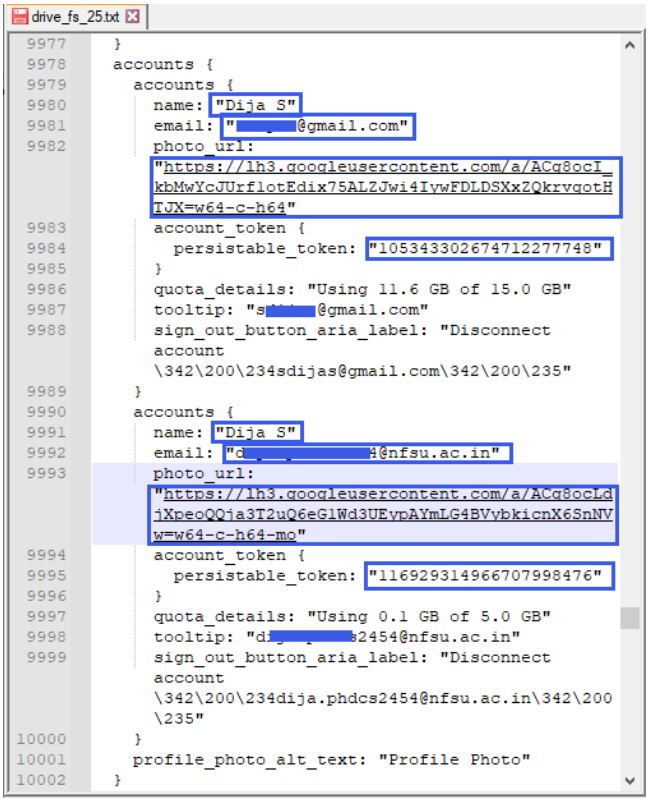


Fig -3: The details of email accounts information stored inside DriveFS files.

From Fig. 1, the GAIA ID of the Default user is identified as "105343302674712277748". This same GAIA ID appears in DriveFS as the persistable_token, which is stored inside the drive_fs_*.txt files. Fig. 3 shows how DriveFS saves the persistable_token for each configured user account. Since the GAIA ID and the persistable_token represent the same unique identifier for a given email account, they can be directly correlated across browser artifacts and DriveFS files.

This unique number provides a reliable way to link the activity traces found in browser files with those found in the locally installed Google Drive App (DriveFS). As shown in Fig. 3, the drive_fs_*.txt files also store additional information such as the user's name, email ID, and even the profile picture URL—all of which may be valuable during an investigation.

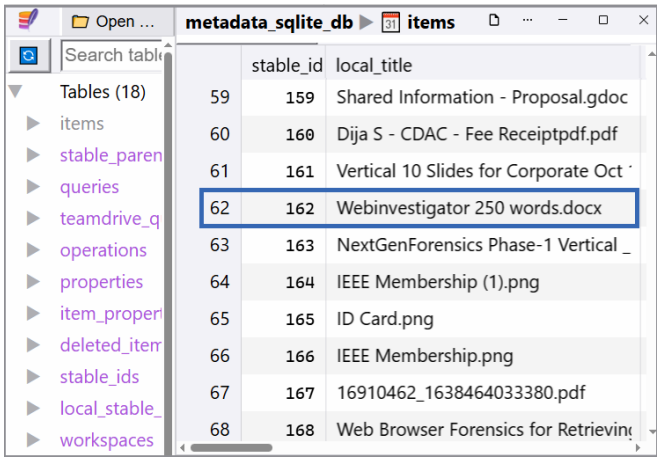


Fig -4: Uploaded/Downloaded Files using the DriveFS

Once the user accounts have been identified, the next step is to extract information about the files uploaded or downloaded through the locally installed Google Drive App (DriveFS). This is done by examining the metadata_sqlite_db file stored locally. Within this database, the "items" table contains the names and details of all files that were uploaded or downloaded using DriveFS as shown in Fig -4. The SQLite database for each user is located in a separate folder, for example:

C:\Users\Admin\AppData\Local\Google\DriveFS\105343302674712277748.

This structure shows that DriveFS creates an individual folder for each user account, named using the user's persistable_token (GAIA ID). Therefore, each account's file activity can be found in its respective metadata_sqlite_db file under that folder. By analyzing the "items" table within each user's DriveFS directory, investigators can clearly separate and attribute Google Drive activities to specific email accounts. This becomes a critical step in accurately identifying the actual suspect in a cybercrime investigation.

2.6 Step by Step Methodology to extract the Google Drive Activities

The steps below describe the process of identifying and correlating Google Drive activities by examining artifacts stored in web browsers and the Google Drive desktop application on Windows OS Systems.

Step 1: Collect browser artifacts

Step 2: Extract all Gmail IDs

Step 3: Extract file details and Drive URLs

Step 4: Collect DriveFS logs

Step 5: Retrieve account details from DriveFS logs

Step 6: Extract file details from DriveFS metadata

Step 7: Correlate browser artifacts with Drive FS data using the 64-bit unique GAIA-ID and persistable-token.

3. CHALLENGES

Cloud and browser forensic investigations come with several challenges, such as the use of incognito modes, manual cookie or history deletion, browser profile resets, multiple simultaneous account logins, VPN-based identity masking, and even tampering with DriveFS directories [1], [3], [6], [8]. In Google Drive forensics on Windows systems, one of the biggest difficulties is the inconsistency and volatility of browser-generated artifacts. Modern browsers frequently change how they store information—whether through updated SQLite schemas, altered cookie management, or redesigned IndexedDB structures— which directly impacts the reliability and stability of forensic extraction. Moreover, users can deliberately or unintentionally erase evidence by clearing browsing data or by using private browsing modes, which removes or suppresses crucial entries such as history logs, cookies, and autofill records. Differences among Chromium-based browsers add yet another layer of complexity: even though many of them share similar foundations, browsers like UC Browser and Yandex exhibit distinct storage behaviors and retain artifacts differently. Because of these variations, investigators cannot always rely on browser artifacts alone to reconstruct a complete and accurate picture of Google Drive activity.

4. FUTURE WORK

Future work should also look into recovering artifacts from volatile, cloud-linked sources such as RAM captures, which may contain temporary authentication data or traces of recent Google Drive activity. Expanding the analysis to mobile platforms like Android and iOS is another important direction, as Google Drive is widely used on smartphones and the artifacts stored on these devices differ greatly from those found on Windows systems. Another valuable area of research is examining how deleted or partially synchronized items can be recovered from DriveFS internals, since these remnants may still hold useful investigative information. In addition, developing advanced forensic tools that can reconstruct partial or deleted artifacts through unallocated disk space and slack space analysis would greatly strengthen evidence recovery—especially in cases where users have intentionally tried to hide their actions. Such tools would help investigators recover traces that traditional methods might miss, ultimately improving the accuracy and effectiveness of Google Drive forensic investigations.

5. CONCLUSION

This research paper presents a unified and practical methodology for identifying Gmail accounts and reconstructing Google Drive activity by correlating browser artifacts with DriveFS metadata. The study demonstrates

that Google Drive interactions carried out on Windows systems leave behind a substantial collection of forensic traces in both web browsers and the Google Drive Desktop Application. Key details—such as Drive URLs, file names, timestamps, and most importantly, the user's identity (email address, profile information, and GAIA ID)—can be successfully recovered from locally stored browser databases, JSON files, and DriveFS logs. Through detailed analysis of SQLite databases, configuration files, and metadata caches, investigators can accurately reconstruct upload, download, and file-access events, even when multiple accounts are involved on the same machine.

The use of the GAIA ID and the DriveFS persistable_token provides a powerful correlation mechanism for reliably linking browser-based user activity with DriveFS-level evidence, enabling precise user attribution. The step-by-step methodology introduced in this study equips investigators with a structured and repeatable approach to determine exactly which Gmail account performed specific Google Drive operations. Overall, the findings highlight the strong forensic value of both browser artifacts and DriveFS data in cybercrime cases involving cloud storage misuse. By offering clear extraction procedures and dependable correlation strategies, this research enhances the effectiveness of digital forensic investigations on Windows systems and contributes meaningfully to the broader field of cloud forensics.

REFERENCES

[1] S. Chung, R. S. Humphries, and A. Clark, "Cloud Storage Forensics: A Survey of Issues and Approaches," Digital Investigation, vol. 44, pp. 1–15,Mar. 2023, doi: 10.1016/j.diin. 2023.301208.

[2] M. Y. Wong and G. Brown, "Forensic Examination of Google Drive File Synchronization Artifacts in Windows 10," Forensic Science International: Digital Investigation, vol. 39, Jun. 2024, pp. 301–315, doi:10.1016/j.fsidi.2024.300152.

[1] A. Ahmed and T. Kechadi, "A Forensic Analysis of Browser-Based Artifacts for Detecting Online Service Abuse," Computers & Security, vol. 124, pp. 102–118, Feb. 2025, doi:10.1016/j.cose.2025.103322.

[2] L. Ruiz, "Forensic Relevance of Google Account Session Cookies across Chromium Browsers," Journal of Digital Forensics, Security and Law, vol. 18, no. 2, pp. 55–75, 2023.

[3] S. Dija, "Browser Forensics of Chromium-Based Web Browsers in Windows Systems International Research Journal of Engineering and Technology (IRJET), vol. 10, Issue: 10, Nov 2024.

[4] J. D. Grimes and P. McCarthy, "Residual Artifacts of Cloud Storage Apps on Windows Systems," Journal of Cyber Forensics and Information Security, vol. 13, no. 1, pp. 21–46, 2024.

[5] A. Qureshi and D. Karabiyik, "An In-depth Forensic Analysis of Chromium-based Browser Autofill Artifacts," Information Security Journal, vol. 33, no. 6, pp. 212–228, 2024, doi:10.1080/19393555.2024.1001159.

[6] P. Mahajan, "Forensic Recovery of Deleted SQLite Records from Browser Databases," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 4601–4615, Dec. 2024, doi:10.1109/TIFS.2024.3378251.

[7] A. R. Alanzi and F. Saleh, "Forensic Investigation of Multi-Account Google Login Artifacts on Windows OS," Journal of Digital Forensics, Security and Law, vol. 19, no. 3, pp. 10–32, 2024.