International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1203-1211

Journal homepage: http://iieta.org/journals/ijsse

Digital Forensics in Google Drive: Techniques for Extracting and Analyzing Digital Artifacts

Erika Ramadhani*, Syafiq Irfan Isnaindar

Department of Informatics, Universitas Islam Indonesia, Yogyakarta 55584, Indonesia

Corresponding Author Email: erika@uii.ac.id

https://doi.org/10.18280/ijsse.140417

Received: 30 October 2023
Revised: 2 July 2024
Accepted: 17 July 2024
Available online: 30 August 2024

Keywords:
digital forensics, digital artifact, forensics cloud, Google Drive, cloud computing

ABSTRACT

The problem of cloud forensics is the difficulty in identifying and accessing evidence log. It also used to store illegal and prohibited content. This research proposes to address this problem by developing a comprehensive activity for investigating Google Drive with digital forensics. We will explore the techniques and methodologies required to uncover digital artifacts within Google Drive by using National Institute of Standards and Technology (NIST) method, covering aspects such as user activity logs, file metadata, document revisions, and access permissions. The NIST method consists of collection, interpretation, and reporting activities. Collection activities include protect, acquire and ensure. Interpretation activities include recover, navigate, identify, and analyze. And reporting activities consist of reporting results and writing reports. The result of this paper is by using the DB Browser tool, the artifact such as activity log, file metadata, document revision, and access permission is not present. Meanwhile when using Magnet Axiom, the evidence is found but not related to the scenario. Our aim is to provide a structured approach that digital forensics experts can employ to navigate Google Drive and extract relevant evidence effectively.

1. INTRODUCTION

In an increasingly digital age, the way individuals and organizations store, access, and share their data has witnessed a significant transformation. Cloud-based platforms, such as Google Drive, have become fundamental tools in our daily lives, offering unmatched convenience and accessibility for users worldwide. These platforms allow individuals and businesses to store and collaborate on a multitude of digital assets seamlessly, thus reducing the reliance on traditional physical storage devices. However, this digital convenience brings with it a unique set of challenges, particularly in the context of digital forensics [1, 2].

The growing reliance on cloud storage platforms, like Google Drive, for data storage and collaboration has created a pressing need for digital forensics experts to adapt to the unique challenges presented by these systems. Digital artifacts within Google Drive, whether it be user interactions, document version histories, or metadata, contain potential evidence that can be crucial in legal cases, investigations, or security breaches. Yet, the methods and tools for effectively investigating Google Drive and extracting this vital digital evidence remain relatively uncharted territory [3, 4].

Some of the major challenges include the complexity of cloud computing systems, the lack of standardization in cloud environments, the difficulty in identifying and accessing evidence in logs, the need to maintain the chain of custody and documentation of digital evidence, and the challenge of presenting technical evidence to a jury with limited knowledge of computer systems [5]. The rapid and widespread adoption of Google Drive and similar cloud storage services has raised concerns regarding their potential misuse for storing illegal or prohibited content [6]. This misuse poses a grave issue for law enforcement agencies, organizations, and the providers themselves, as the cloud's anonymity and accessibility can inadvertently foster illicit activities [7].

To address the problem of misleading use of Google Drive for illegal file storage, we propose the application of NIST framework for digital forensics. The NIST framework offers a structured and systematic approach to digital investigations, enabling the identification and analysis of digital artifacts within Google Drive. This approach encompasses data acquisition, preservation, examination, analysis, and reporting, with a focus on maintaining the integrity and legality of the evidence collected [8-11].

This research proposes to address this problem by developing a comprehensive activity for investigating Google Drive with digital forensics. We will explore the techniques and methodologies required to uncover digital artifacts within Google Drive, covering aspects such as user activity logs, file metadata, document revisions, and access permissions. Our aim is to provide a structured approach that digital forensics experts can employ to navigate Google Drive and extract relevant evidence effectively.

This research embarks on an exploration of Google Drive as a case study in digital forensics. Our investigation aims to uncover the hidden digital artifacts within Google Drive, which can provide invaluable insights for digital forensic experts, legal professionals, and individuals concerned with data security and privacy. By delving into the intricacies of Google Drive's architecture, data storage methods, and the traces left behind during user interactions, we aspire to gain a comprehensive understanding of its forensic potential.

2. LITERATURE REVIEW

Lim et al. [12] examined the forensic implications of the Dropbox cloud storage service, which can be misused to store illegal or prohibited content. Method used is examination of the Dropbox client application on a Windows 10 system and identification of relevant forensic artifacts from both the local system and the Dropbox cloud storage provider.

Bowers et al. [13] proposed a system to detect suspicious file migration or replication in cloud storage services. it proposes a system called LAST-HDFS that integrates Location-Aware Storage Technique (LAST) into the open source Hadoop Distributed File System (HDFS) to enforce location-aware file allocations and continuously monitor file transfers to detect potentially illegal transfers in the cloud. Main findings are the LAST-HDFS system was implemented and evaluated in a large-scale real cloud environment, the system uses algorithms to model file transfers and store data with similar privacy preferences in the same region and the system uses socket monitors to monitor real-time communication between cloud nodes and calculates the probability of a file transfer being illegal.

Ali et al. [14] analyzed cloud forensics techniques and their practical challenges/limitations for investigating cyber-attacks in cloud environments. Method of the paper is review and analysis of cloud forensics techniques and their practical challenges/limitations, examination of the complexities and challenges involved in collecting digital evidence in cloud environments, and exploration of how collected evidence can be used for investigations and to improve cloud security.

Pawlaszczyk et al. [15] provided an overview of the state of research on cloud forensics, discusses the technical and legal challenges of acquiring forensic evidence from cloud services, and introduces an API-based approach to acquiring evidence from cloud services as well as a proof-of-concept framework called CLOUDxTRACT. Method of this paper providing an overview of the existing research on forensic evidence acquisition from cloud services, identifying and discussing the technical and legal challenges involved in this process, comparing different basic techniques for acquiring data from the cloud, using 30 cloud storage services as examples, introducing and evaluating an API-based evidence acquisition approach, where the authors utilize the officially supported APIs of cloud services to acquire forensic data, and presenting a proof-of-concept framework called CLOUDxTRACT, which they use to acquire evidence from selected cloud service providers.

Jeyamohan [16] presents the results of the case simulation of securing Samsung Galaxy A8 brand android smartphone evidence using the NIST method and MOBILedit Forensic Express tool. The data backup, extraction, and analysis of the smartphone using the NIST method and MOBILedit Forensic Express tool resulted in findings sought for investigation and evidence of crimes committed by persons using android smartphone facilities. The paper also includes a reporting stage that provides a description of the case, the tool and procedure used, actions taken, and recommendations for policy, procedure, and other aspects of forensic.

3. METHOD

3.1 NIST method

The aim of this research is to identify user data artifacts accessed through Goolge Drive on desktop application and to provide recommendations for improving policies, methods, tools, or other supportive aspects of the digital forensics process. The research consists of three stages: Collecting, interpretation, and reporting. The NIST method is used in the analysis phase to ensure that the discovered data is indeed unique and authentic, in accordance with the evidence at the scene of the incident [17, 18]. The results of the digital data analysis are subsequently referred to as digital evidence, which must be scientifically and legally accountable [19].

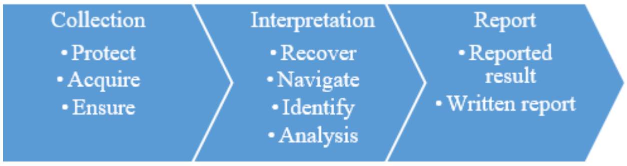


Figure 1. Steps of digital investigation

From Figure 1, we can see:

Collection: the collection stage of a digital investigation involves the collection of potential evidence, which may include computers, mobile devices, storage devices, copies of data from cloud accounts, and other sources. The collection steps ensure the integrity of the acquired evidence to provide a stable source for the analysis of the data and, if possible, protect the original data from accidental modification during the acquisition [20, 21].

Interpretation: the interpretation stage of a digital investigation is the process of analyzing and making sense of the collected evidence to draw conclusions about the case. This stage involves examining the evidence in detail, identifying patterns and relationships, and developing a narrative that explains what happened. The interpretation stage requires a deep understanding of the technology and tools used to collect and analyze the evidence, as well as the ability to apply critical thinking and analytical skills to the data. It is important to note that the interpretation stage is not just about analyzing the evidence itself, but also about considering the broader context of the case, such as the legal and ethical implications of the findings. The goal of the interpretation stage is to provide a clear and accurate picture of what happened, which can be used to support legal or other actions related to the case [22].

Reporting: the reporting stage of a digital investigation is the process of documenting the findings of the investigation in a written report. This report is typically the final product of the investigation and is used to communicate the results to stakeholders such as law enforcement, legal teams, or other interested parties. The report should be clear, concise, and accurate, and should include a detailed description of the investigation process, the evidence collected, and the conclusions drawn from the evidence. The report should also include any relevant legal or ethical considerations, as well as recommendations for further action if necessary. The goal of the reporting stage is to provide a comprehensive and objective summary of the investigation that can be used to support legal or other actions related to the case. It is important to note that the reporting stage is not just about presenting the findings of the investigation, but also about ensuring that the report is admissible in court and meets any other legal or regulatory requirements [23].

3.2 5W1H framework

The 5W1H framework is based on the Occam Razor and Alexiou Principles. On the principle that Occam razor thinks that wisdom is done by simply explaining is a better thing. To solve a case requires simple and simple steps. The principle of Alexiou's view consists of four questions:

1. What question are you trying to answer?
2. What data do you need to answer that question?
3. How do you extract/analyze that data?
4. What does the data tell you?

In the digital forensic investigation process, the principle that can be used is 5W1H which covers what, where, when, why, who, and how.

3.3 Scenario

This scenario is created to provide an overview of cybercrime activities within the scope of Google Drive cloud computing. In this scenario depicted in Figure 2, the perpetrator of the crime uses a laptop to access cloud computing, which is used as a location for storing data and files that are utilized in criminal activities. In this scenario, the perpetrator stores several documents related to the crime and photos taken during the criminal activities with the intention of avoiding the use of physical evidence if caught. The files stored by the perpetrator in Google Drive are eventually deleted, and these files are in PDF, doc, jpg, and txt formats. The laptop used by the researcher will be depicted as the evidence obtained, and the researcher will play the role of the investigator in this scenario.

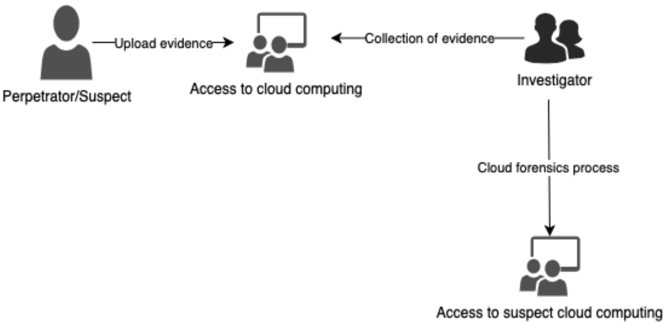


Figure 2. Scenario

The forensic process by itself will follow the NIST guidelines on forensic methods as described above. To that extent, the researcher has also prepared some tools for supporting the forensic process such as imaging tools, data acquisition tools, and tools for database access. Moreover, it begins with the collection phase in which tries to access the folder location suspected to contain Google Drive artifacts at the path C:\Users\ACER\AppData\Local\Google\DriveFS in search of key Google Drive artifacts such as sync_config.db, snapshot.db, and sync_log.db. The artifacts found on the mentioned path are examined by making hash values to keep the integrity of the artifacts so their condition does not change. The analysis stage where the findings analyzed make it easier to create a report on the ongoing forensic process. Analysis will be based on the evidence collected during the forensic process in the form of the screenshots from tools and what is observed. The final step is the reporting phase, where a report is created regarding the results or findings obtained. This report comprises information on the artifacts found and the tools used, and also encompasses results of analysis using screenshots with further explanations presented in a tabulated form.

4. RESULT AND DISCUSSION

Before the data collection phase is carried out, the researcher records the software and tools used during the digital forensic process shown in Table 1.

Table 1. List of software for conducting cloud forensics

Software	Description
Laptop Acer Aspire 5 A514-51G-52M2	Media for conduction digital forensics
Google Drive Desktop Version: 66.0.3.0	Cloud storage
Magnet Axiom Process	Tool for capturing and imaging
DB Browser for SQLite Version 3.12.2	Tool to open database file format
FTK Imager	Tool for access hash value

4.1 Collection

4.1.1 Protect

Research was conducted using direct access to Google Drive using existing forensic tools, Google Drive itself is a version of File Stream with Mirror files mode where files uploaded into Google Drive themselves can be accessed offline. However, at the time of direct accessing Google Drive, the forensics tools used can not detect, so the forensic process is redirected by accessing the folder path described earlier. The objective of this activity is to protect the data.

Table 2. List of main artifact on Google Drive

File	Description
sync_config.db	The SQLite file that provides you with information about the connected Google Drive account and the location of the synchronization folder.
snapshot.db	The SQLite file that contains a list of files known by Google Drive and their actions being monitored in the synchronization folder. This log includes some interesting information such as file hashes, names, Google IDs, and timestamps.
sync_log.db	A text file containing a lot of information about events that have occurred in Google Drive, including events of creation, deletion, and modification.

4.1.2 Acquire

The experiment was conducted by trying to access the location of some of the artifacts from Google Drive itself. The researchers tried to find some artifact such as sync_config.db, snapshot.db and sync _log.db by accessing path folders or accessing location from

C:\Users\ACER\AppData\Local\Google\DriveFS. As for the above-mentioned archives, when accessed, they contain some information about the Google Drive accounts that are synchronized on the device.

The mentioned artifact files listed in Table 2, when accessed, contain various information about the synchronized Google Drive account on the device. The reason for choosing files in the db format over other file types is the hope that these db files contain detailed information about the Google Drive used in the research.

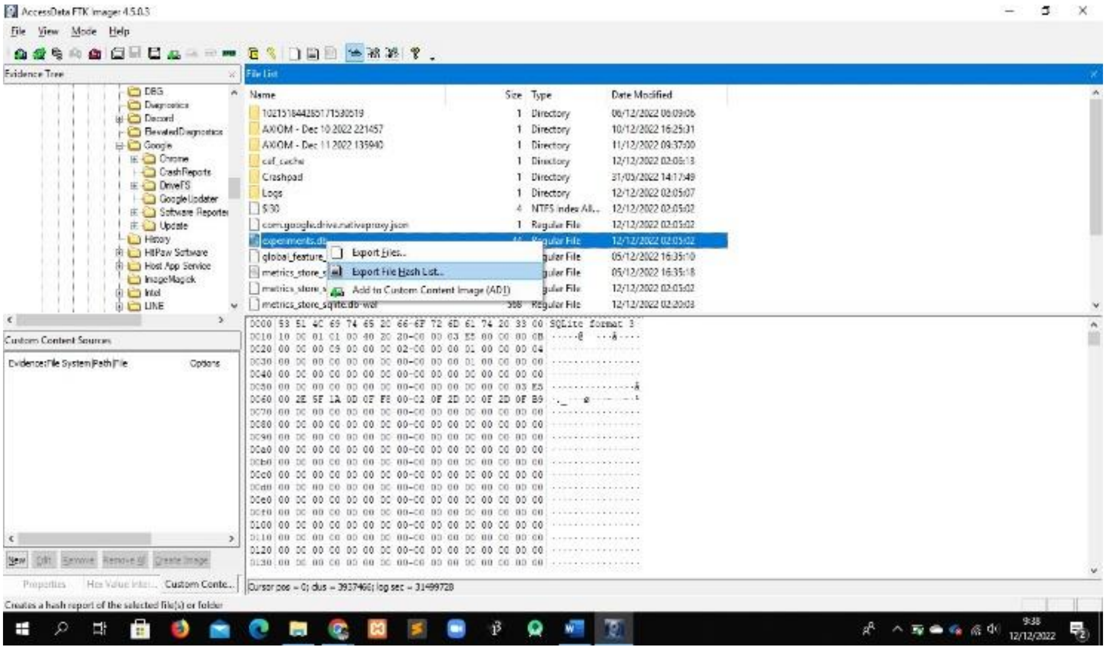
However, at the time the location was accessed, some of the above-mentioned artifacts were not found. As for the database files found, among others experiments.db, metrics_store_sqlite.db and root_preference_squite.db. Since the searched file was not found, it was eventually proceeded to open the contents of the database file with DB Browser tools against each of the files. However, before opening the contents of the file, a hash value is taken from the file to prevent the file from changing its integrity using FTK Imager.

4.1.3 Ensure

To prevent the obtained artifact file from changing its integrity, so it is done with the hash value process. Taking the hash value itself is done using tools FTK Imager by setting the evidence tree on the tool display to the path folder C:\Users\ACER\AppData\Local\Google\DriveFS (see Figure 3).

The first file to take hash value is the experiments.db file depicted in Figure 4. This file itself after taking hash value with tools is obtained value 29cce74dc1aa0f1f36862c0787cfe046 for MD value 5 while the value of SHA-1 is 56e2e9c52cd3a00f63f200691a8be211065fdd7a.

The data for second and third file are summarized in the Table 3. Those three files use Microsoft Excel to open a csv file containing hash value information.



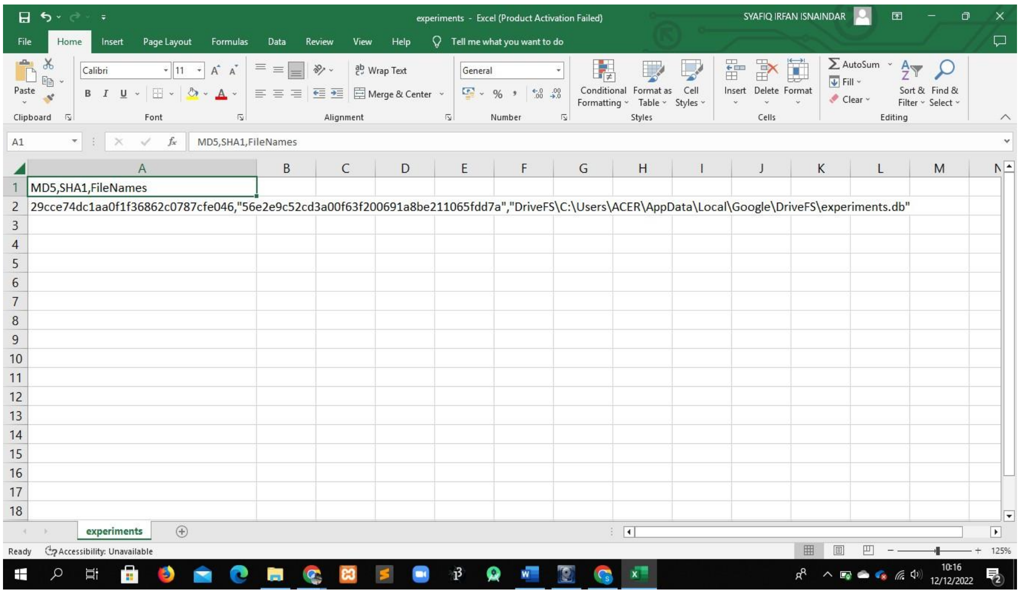
Name	Size	Type	Date Modified
10215184428517 1530619	1	Directory	06/12/2022 06:09:06
AXIOM - Dec 10 2022 221457	1	Directory	10/12/2022 16:25:31
AXIOM - Dec 11 2022 135940	1	Directory	11/12/2022 09:37:00
cef_cache	1	Directory	12/12/2022 02:05:13
Crashpad	1	Directory	31/05/2022 14:17:49
Logs	1	Directory	12/12/2022 02:05:07
$I30	4	NTFS Index All...	12/12/2022 02:05:02
com.google.drive.nativeproxy.json	1	Regular File	12/12/2022 02:05:02
experiments.db	44	Regular File	12/12/2022 02:05:02
global_feature_		Regular File	05/12/2022 16:35:10
metrics_store_s		Regular File	05/12/2022 16:35:18
metrics_store_s		Regular File	12/12/2022 02:05:02
metrics_store_sqlite.db-wal	398	Regular File	12/12/2022 02:20:03

```
0000  53 51 4C 69 74 65 20 66-6F 72 6D 61 74 20 33 00  SQLite format 3
```

Cursor pos = 0; clus = 3937466; log sec = 31499728

Creates a hash report of the selected file(s) or folder

Figure 3. Process of retrieving hash value using FTK Imager



	A
1	MD5,SHA1,FileNames
2	29cce74dc1aa0f1f36862c0787cfe046,"56e2e9c52cd3a00f63f200691a8be211065fdd7a","DriveFS\C:\Users\ACER\AppData\Local\Google\DriveFS\experiments.db"

Figure 4. Hash value files experiments.db accessed with Microsoft Excel

Table 3. List of hash value

File	MD5	SHA-1
sync_config.db	29cce74dc1aa0f1f36862c0787cfe046	56e2e9c52cd3a00f63f200691a8be211065fdd7a
snapshot.db	3b990a23941c7664524e6404bced96c5	c7d31f8d4c40211cd3bacb5fc5b07df68fda0cf2
sync_log.db	40f791ed4b38b59404d145557441bda1	7ab6b6b0647b7865288fa4a74c850b04515fec6e.

4.2 Interpretation

4.2.1 Recover

At this stage, the recovery process is carried out by accessing previously obtained database files, namely (1) experiments.db, (2) metric_store_sqlite.db, and (3) root_preference_squite.db, using the DB Browser to view the contents. This process involves opening the files and searching for the information contained therein. Additionally, the Axiom Magnet tool is also used to analyze DriveFS folders with the aim of finding digital artifacts associated with Google Drive information. Using axiom magnet, various digital evidence can be identified and further analyzed to find data relevant to this investigation.

4.2.2 Navigate

At the navigate stage, the activity is performed by browsing the contents of the database files experiments.db, metric_store_sqlite.db, and root_preference_squlite. db using the DB Browser to identify the data or values stored therein. This process also includes navigation to the location of the folder on the computer (`C:\Users\ACER\AppData\Local\Google\DriveFS`) to access the required database files. In addition, the Axiom Magnet tool is used to navigate various categories of evidence such as Web Related, Media, Documents, and Operating System found in the DriveFS folder, allowing for more in-depth digital evidence search and identification.

4.2.3 Identify

At the identification stage, the activity is performed by identifying and recording the contents of each key in the experiments.db file, such as the BLOB value, the "set" text, the value "NAK102151844285171530519," and the code on the portablephenotype_zwieback_impl_cookie_key. In addition, empty results were identified on files metric_store_sqlite.db and root_preference_squlite. db, which did not contain specific information related to Google Drive. The researchers also used the Axiom Magnet to identify digital artifacts found in Web Related, Media, Documents, and Operating System categories relevant to the Google Drive, helping to determine which artefacts are important for further analysis.

4.2.4 Analysis

In this stage, the research is carried out by accessing the contents of the files obtained earlier using the DB Browser tool as figured in Figure 5. This process is aimed at accessing the information that can be obtained from the previously discovered database files. The first file accessed is experiments.db to view its contents, and the results are displayed in the Table 4.

In the "registered_package/drive_fs_ph" key with a BLOB value, when clicked, it only displays a binary number. Moving on to the second key, "portablephenotype_client_storage_reset_version_key_2," it only shows the word "set" without any other information. The third key, "account_ids," in the tool's values displays a dot, and when clicked, it reveals the value "NAK102151844285171530519."

Next, for the fourth and fifth keys, "uncommitted_packages/drive_fs_ph/" and "uncommitted_packages/drive_fs_ph/102151844285171530519," they display BLOB values, and when clicked, they show only binary numbers.

The sixth key, "portablephenotype_zwieback_impl_cookie_key," displays a code-like value that cannot be accessed. Finally, the seventh value, "last_sync," displays a number with a value of 1670723270.

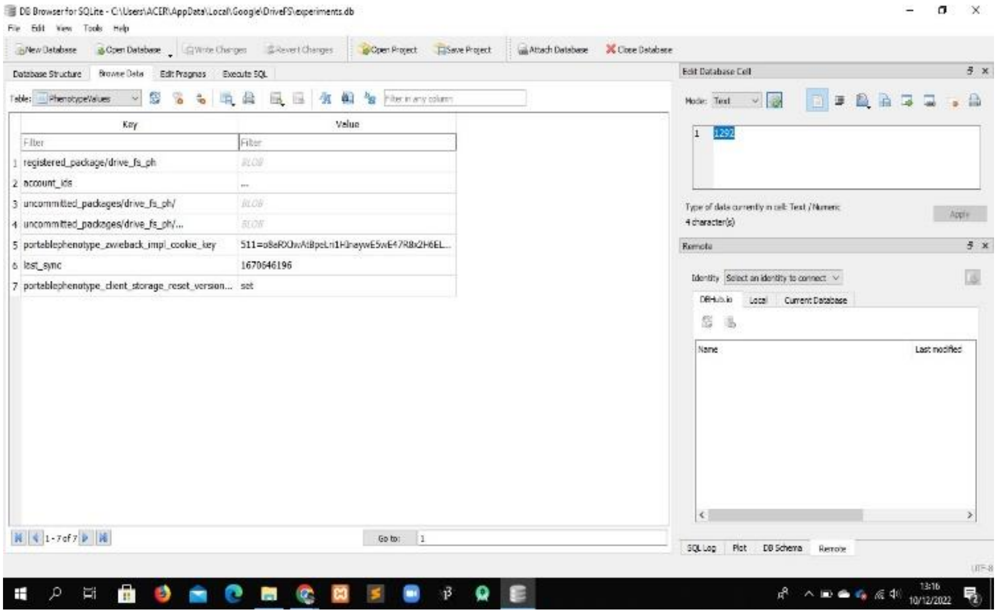

DB Browser for SQLite - C:\Users\ACER\AppData\Local\Google\DriveFS\experiments.db

Table: PhenotypeValues

	Key	Value
1	registered_package/drive_fs_ph	BLOB
2	account_ids	...
3	uncommitted_packages/drive_fs_ph/	BLOB
4	uncommitted_packages/drive_fs_ph/...	BLOB
5	portablephenotype_zwieback_impl_cookie_key	511=o8eRXQwAtBpeLn1H3naywE5wE47R8x2H6EL...
6	last_sync	1670646196
7	portablephenotype_client_storage_reset_version...	set

Edit Database Cell

Mode: Text

1 1292

Type of data currently in cell: Text / Numeric

4 character(s)

Identity: Select an identity to connect

1 - 7 of 7

Go to: 1

Figure 5. Experiments.db artifact accessed with DB Browser

Unfortunately, the experiments.db file itself does not contain any related information such as account details, email, password, account activities, or other information.

Next, access the next file, namely the metric_store_sqlite.db file, which has a capacity of 12 KB and is in the folder path mentioned earlier, which is in the path C:\Users\ACER\AppData\Local\Google\ DriveFS. The access process is carried out in the same way, using the DB Browser tool, by clicking the "Open Database" menu and then directing it to the folder location where the metric_store_sqlite.db file is located, and then clicking on that file.

The result was that no key was found when accessing the metric_store_sqlite.db file, and there was no value associated with the file. Only an empty table with no specific information about Google Drive was present. After that, access was made to the next file, which is the root_preference_sqlite.db file. By following the same process and steps, the file only displayed information in the form of an id_type with a max_root_id value of 3 without providing specific information about Google Drive itself.

The researcher proceeded to analyze digital evidence using Magnet Axiom tools in the DriveFS folder with the hope of finding other artifacts related to Google Drive information. Magnet Axiom detected several pieces of evidence within the scope of Web Related, Media, Documents, and Operating System. These pieces of evidence were marked with green tags using Magnet Axiom tools depicted in Figure 6.

4.3 Reporting

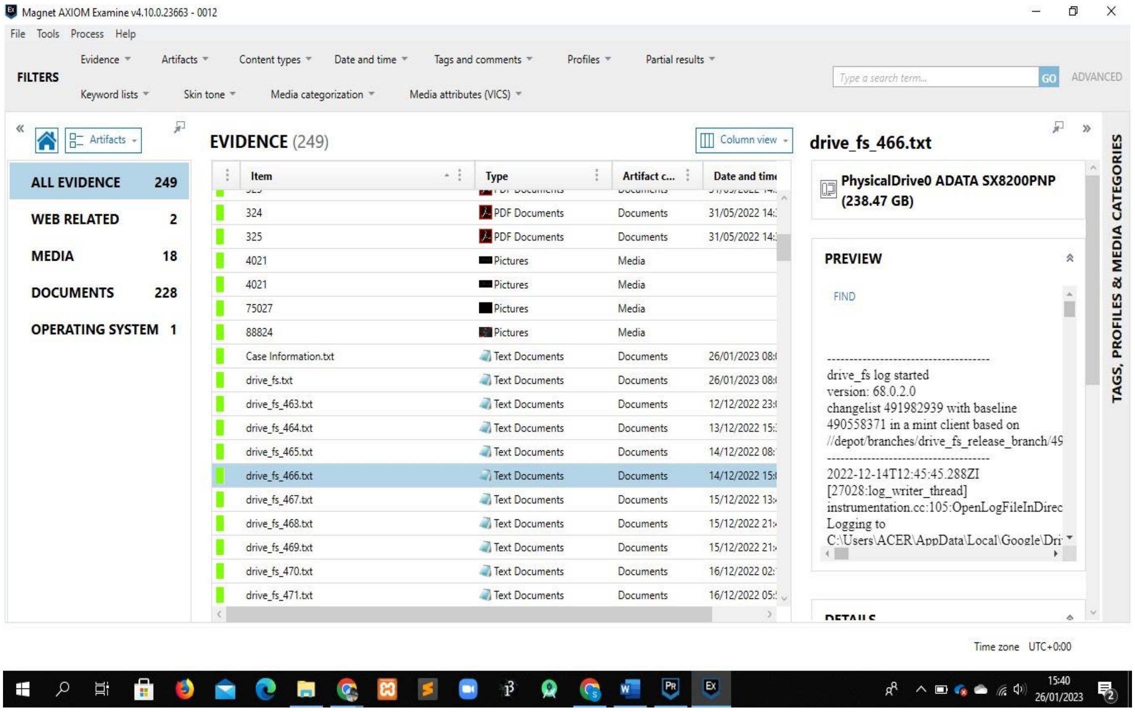
The report obtained with Magnet Axiom tools after the analysis process in the DriveFS folder reveals a total of 237 pieces of evidence obtained using the tools as summary in Table 5.

The artifacts in the Table 6 are database artifacts, and during the research, the researcher initially believed that these artifacts would contain information about Google Drive accounts. However, after accessing them with DB Browser, it turned out that the information visible had no relevance to Google Drive accounts at all. In fact, one of the artifacts contained no information at all.

We use the 5W+1H approach, with the details of Who, What, When, Where, Why, and How explained in the following Table 7.

Table 4. Results of accessing the experiments.db file with DB Browser

No.	Key	Value
1	registered_package/drive_fs_ph	BLOB
2	portablephenotype_client_storage_reset_version_key_2	set
3	account_ids	…
4	uncommitted_packages/drive_fs_ph/	BLOB
5	uncommitted_packages/drive_fs_ph/102151844285171530519	BLOB
6	portablephenotype_zwieback_impl_cookie_key	511=CtCJX4i7tgaeMVl9adJbb70TX8wPAOzWVKUCO_Gxca9GHWFCP9EsBNyfloRrFwtTe2hEcxSqopq5cSlI8iovk2Xp-FmtpZJB2sp4JjcuVzThMpcAPh3dR12N0N1RTm47KfRo2-luPyLdufAan85L45w73gUWVSnW-p-Uk70GK5k
7	last_sync	1670723270



ALL EVIDENCE	249
WEB RELATED	2
MEDIA	18
DOCUMENTS	228
OPERATING SYSTEM	1

EVIDENCE (249)

Item	Type	Artifact c...	Date and time
324	PDF Documents	Documents	31/05/2022 14:
325	PDF Documents	Documents	31/05/2022 14:
4021	Pictures	Media	
4021	Pictures	Media	
75027	Pictures	Media	
88824	Pictures	Media	
Case Information.txt	Text Documents	Documents	26/01/2023 08:
drive_fs.txt	Text Documents	Documents	26/01/2023 08:
drive_fs_463.txt	Text Documents	Documents	12/12/2022 23:
drive_fs_464.txt	Text Documents	Documents	13/12/2022 15:
drive_fs_465.txt	Text Documents	Documents	14/12/2022 08:
drive_fs_466.txt	Text Documents	Documents	14/12/2022 15:
drive_fs_467.txt	Text Documents	Documents	15/12/2022 13:
drive_fs_468.txt	Text Documents	Documents	15/12/2022 21:
drive_fs_469.txt	Text Documents	Documents	15/12/2022 21:
drive_fs_470.txt	Text Documents	Documents	16/12/2022 02:
drive_fs_471.txt	Text Documents	Documents	16/12/2022 05:

drive_fs_466.txt

PhysicalDrive0 ADATA SX8200PNP (238.47 GB)

PREVIEW

```
-----------------------------------
drive_fs log started
version: 68.0.2.0
changelist 491982939 with baseline
490558371 in a mint client based on
//depot/branches/drive_fs_release_branch/49
-----------------------------------
2022-12-14T12:45:45.288ZI
[27028:log_writer_thread]
instrumentation.cc:105:OpenLogFileInDirec
Logging to
C:\Users\ACER\AppData\Local\Google\Dri
```

Figure 6. Tagging process for all found evidence

Table 5. Report on imaging results with Magnet Axiom

Evidence Finding	Description	Total
Web Related	One of the two pieces of evidence displays a link that accesses Google Drive help services, while the other link cannot be accessed.	2
Media	The artifact found is an image with additional information such as size, location, hash value, etc.	18
Documents	The artifacts found are in PDF and text formats, containing information such as when the file was last created, accessed, and modified, along with the file's location, hash value, evidence number, recovery method, and more.	216
Operating System	It only displays native items with information such as the file's location, without showing any information related to Google Drive itself.	1

Table 6. Analysis reports with DB Browser

Artefact	Description
experiments.db	After accessing it, it displays seven keys, each of which has a different value.
metric_store_sqlite.db	After accessing it, it is empty, and no information is obtained.
root_preference_sqlite.db	It only displays two items, namely id_type and value.

Table 7. 5W + 1H regarding the results of the forensic process

Coverage	Question	Description
Who	Who was involved?	A perpetrator with laptop evidence and the role of the researcher is based investigators scenario.
What	What did the perpetrator do? What is got it?	The perpetrator uploaded several documents to do crime on Google Drive, investigators found some documents from investigation with tools Axiom magnets are in the form of images, PDF and txt files.
When	When did the perpetrator take action?	Based on the findings investigators with tools shows the time different. However, the perpetrator accessed it using Google Drive occurs on a range March 2022 until December 2022.
Where	Where did the event take place?	Location not found.
Why	Why did the perpetrator do this?	The perpetrator uses Google Drive to avoid finding physical evidence if caught.
How	How investigators carry out the process forensics?	Investigators use NIST forensic methods are appropriate with rules and steps too using tools supporters like DB browser, FTK Imager, Axiom Magnets.

Unfortunately, the researcher did not find any documents directly related to the scenario they created. Many empty files and files that were not actually part of the designed scenario were processed during the analysis and imaging. Some image files were also not processed 100%, with only a portion of the images being processed. Furthermore, the text files that appeared with Magnet Axiom tools were not part of the scenario files, instead, they contained random code-like information. The processed PDF files were also not part of the scenario files prepared for the forensic process. Most of the files processed in the imaging itself came from outside the folder that the researcher had set up to run the scenario, and they were inadvertently included in the analysis process.

In the research, there was an attempt to repeat the process using Magnet Axiom tools, but it still only found PDF, text, and image files that were not part of the scenario. These files resulted from the analysis and imaging with Magnet Axiom tools, but they were not files associated with the research scenario.

The inconsistencies between the expected documentation and the findings at the reporting stage indicate some potential problems. First, it may be related to the design of experiments, especially the selection of files and tools used for analysis. Files experiments.db, metric_store_sqlite.db and root_preference_squite.db are expected to contain relevant information but do not provide useful data. This inconsistency may indicate a discrepancy between the type of data stored in the files and the data required for the investigation. Besides, the limitations of the tools used can also play a role; although Magnet Axiom and FTK Imager are powerful forensic tools, they may not be most suitable for this specific scenario or the latest version of Google Drive File Stream. Researchers should consider these aspects and explore alternative tools or methodologies that may be more appropriate to the specific characteristics of the data being investigated.

Considering the results obtained, live forensics was conducted to verify whether the NIST forensic method is suitable for conducting digital forensics on Google Drive. The process involved capturing RAM, during which the desktop version of Google Drive was in a logged-in state, and in mirror files mode, allowing files in Google Drive to be accessed offline.

5. CONCLUSION

The research above was conducted based on the NIST forensic method, where each step was explained according to the established procedure and scenario. From the results of the research conducted, the author did not find the artifacts that should be present in the Google Drive folder location. Some of the artifacts that the researcher found turned out to be empty, with no information that could be obtained when accessed with DB Browser tools. Furthermore, the researcher conducted imaging with Magnet Axiom tools in the hope of finding files directly related to Google Drive. However, Magnet Axiom tools analyzed artifact files in the form of images, PDF documents, and text files, which were not related to the ongoing research scenario, and no other important files were found. According to the researcher, based on the results obtained, the NIST forensic method may not be suitable for conducting digital forensics on Google Drive. The researcher argues that the Google Drive version used, which is Google Drive File Stream, may have influenced the artifact files found, given that the files obtained were unrelated to the research.

Research results show that although digital forensic investigations cover various types of files and devices, the lack of standard output formats poses significant challenges. This inconsistency makes it difficult to share information and integrate, which ultimately weakens cyber security. By implementing a 5W1H-based framework, the study proposes solutions to normalize digital forensic information, thereby improving clarity and accuracy in sharing information. Further research should focus on developing tools that automatically convert forensic data to 5W1H format, evaluate compatibility with existing tools and standards, and conduct extensive case studies to assess their practical effectiveness in real-world investigations.

ACKNOWLEDGMENT

This work is supported by the Department of Informatics at Universitas Islam Indonesia.

REFERENCES

[1] Mandal, P., Rajput, I. (2023). Cloud forensics: Exploring the challenges and mapping out solutions for the future. International Journal for Research Trends and Innovation, 8(4): 1259-1266. https://doi.org/10.13140/RG.2.2.18945.53605

[2] Quick, D., Choo, K.K.R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? Digital Investigation, 10(3): 266-277. https://doi.org/10.1016/j.diin.2013.07.001

[3] Chang, M.S. (2016). Forensic analysis of Google Drive on windows. International Journal of Innovative Science, Engineering & Technology, 3(8): 324-331.

[4] Aminnezhad, A., Dehghantanha, A., Abdullah, M.T., Damshenas, M. (2013). Cloud forensics issues and opportunities. International Journal of Information Processing and Management, 4(4): 76-85. https://doi.org/10.4156/ijipm.vol4.issue4.9

[5] Simou, S., Kalloniatis, C., Kavakli, E., Gritzalis, S. (2014). Cloud forensics: Identifying the major issues and challenges. In Advanced Information Systems Engineering: 26th International Conference, CAiSE 2014, Thessaloniki, Greece, pp. 271-284. https://doi.org/10.1007/978-3-319-07881-6_19

[6] Hu, G., Li, H., Xu, G., Ma, X. (2023). Enabling simultaneous content regulation and privacy protection for cloud storage image. IEEE Transactions on Cloud Computing, 11(1): 111-127. https://doi.org/10.1109/tcc.2021.3081564

[7] Maskun, M., Anwar, R.N. (2021). Regulation and protection of cloud computing: literature review perspective. Jambura Law Review, 3(2): 336-364. https://doi.org/10.33756/jlr.v3i2.10639

[8] NIST cloud computing forensic science challenges. https://csrc.nist.gov/pubs/ir/8006/final, accessed on Aug. 06, 2024.

[9] Goggi, S., Pardelli, G., Bartolini, R., Monachini, M. (2019). Semantic query analysis from the global science gateway. Grey Journal, 15(3): 147-155. https://doi.org/10.6028/NIST.SP.800-145

[10] Umar, R., Riadi, I., Muthohirin, B.F. (2018). Acquisition of email service based android using NIST. KINETIK: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 3(3): 263-270. http://doi.org/10.22219/kinetik.v3i4.637

[11] Breese, J.L., McKeesport, P.A., Roshanaei, U.M., Abington, P.A., Gardner, U.B., Haven, S., Landmesser, U.J.A. (2023). Digital forensics and incident response (DFIR): A teaching exercise. In Proceedings of the ISCAP Conference, Albuquerque, NM, USA, pp. 4901. http://doi.org/10.6028/NIST.IR.8354

[12] Lim, S.Y., Johan, A., Daud, P., Ismail, N.A. (2020). Dropbox forensics: Forensic analysis of a cloud storage service. International Journal of Engineering Trends and Technology, 45-49. https://doi.org/10.14445/22315381/cati3p207

[13] Bowers, A., Liao, C., Steiert, D., Lin, D., Squicciarini, A., Hurson, A. (2021). Detecting suspicious file migration or replication in the cloud. IEEE Transactions on Dependable and Secure Computing, 18(1): 296-309. https://doi.org/10.1109/tdsc.2018.2885271

[14] Ali, S.A., Memon, S., Sahito, F. (2020). Analysis of cloud forensics techniques for emerging technologies. In 2020 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), Tirana, Albania, pp. 106-111. https://doi.org/10.1109/contesa50436.2020.9302862

[15] Pawlaszczyk, D., Bochmann, M., Engler, P., Klaver, C., Hummert, C. (2022). API-based evidence acquisition in the cloud - a survey. Open Research Europe, 2: 69. https://doi.org/10.12688/openreseurope.14784.1

[16] Jeyamohan, N. (2017). Android digital forensics-simplifying android forensics using regular expressions. In 2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer), Colombo, Sri Lanka, pp. 1-1. https://doi.org/10.1109/ICTER.2017.8257836

[17] Guttman, B., Laamanen, M.T., Russell, C., Atha, C., Darnell, J. (2022). Results from a black-box study for digital forensic examiners. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/nist.ir.8412

[18] Hariyadi, D., Kusuma, M., Sholeh, A. (2021). Digital forensics investigation on Xiaomi smart router using SNI ISO/IEC 27037: 2014 and NIST SP 800-86 framework. In International Conference on Science and Engineering (ICSE-UIN-SUKA 2021), pp. 143-147. https://doi.org/10.2991/aer.k.211222.023

[19] Prayudi, Y., Ashari, A., Priyambodo, T.K. (2014). Digital evidence cabinets: A proposed framework for handling digital chain of custody. International Journal of Computer Applications, 107(9): 30-36.

[20] Kent, K., Chevalier, S., Grance, T., Dang, H. (2006). Guide to integrating forensic techniques into incident response. Special Publication (NIST SP) - 800-86. https://doi.org/10.6028/NIST.SP.800-86

[21] Prasetyo, B., Toha, L.Q., Retnani, W.E.Y. (2023). Risk management using COBIT 5 for risk: A case study on local government in Indonesia. Kinetik: Game Technology, Information System, Computer Network,

Computing, Electronics, and Control, 8(1): 435-444. https://doi.org/10.22219/kinetik.v8i1.1585

[22] Gunawan, C.T.A., Suryanto, Y. (2022). Maturity level analysis of digital evidence handling on integrated criminal justice system based on NIST SP800-53 revision 5 using NIST maturity. Budapest International Research and Critics Institute-Journal, 5(2): 10481-10497. https://doi.org/10.33258/birci.v5i2.4861

[23] Ramadhan, R.A., Setiawan, P.R., Hariyadi, D. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037: 2012 and NIST SP800-86 framework. IT Journal Research and Development, 6(2): 162-168. https://doi.org/10.25299/itjrd.2022.8968