

Cloud Storage Forensics

Dissertation submitted
to
RASHTRIYA RAKSHA UNIVERSITY
(*An Institution of National Importance*)

For the partial fulfilment for the award of the degree of

M.Sc in Cybersecurity and Digital Forensics

Submitted by

GONDALIYA PARTH VINODBHAI
(240031102551037)

Under the Guidance of

DR. NITIN PADARIYA

Assistant Professor,

School of Information technology, Artificial intelligence and Cybersecurity



**SCHOOL OF INFORMATION TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND
CYBERSECURITY**

RASHTRIYA RAKSHA UNIVERSITY,

Lavad, Dehgam, Gandhinagar-382305, Gujarat, India

November 2025

DECLARATION

The work embodied in this Dissertation titled “**Cloud Storage Forensics**” submitted for the partial fulfillment of the degree of **M.Sc in Cybersecurity and Digital Forensics** is the original research work carried out by me. The research work does not form the basis for the award of any degree, diploma, associateship, fellowship or other titles in the Rashtriya Raksha University or similar institutions of higher learning. All the ideas and references have been duly acknowledged.

Parth Gondaliya

Date: 17/11/2025

CERTIFICATE

This is to certify that the Dissertation titled "**Cloud Storage Forensics**" was carried out by **Gondaliya Parth Vinodbhai (Enrollment no : 240031102551037)** studying at **School of Information Technology, Artificial Intelligence and Cybersecurity** for partial fulfillment of **M.Sc in Cybersecurity and Digital Forensics** degree to be awarded by Rashtriya Raksha University. This research work has been carried out under my guidance and supervision and it is up to my satisfaction. The Dissertation is fit to be considered for evaluation for the degree of **M.Sc in Cybersecurity and Digital Forensics.**

Date: 17/11/2025

Place: RRU, Gandhinagar

Dr. Nitin Padariya
Assistant Professor

Dr. Chandresh Parekha
Director I/c
SITAICS

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to everyone who contributed to the successful completion of this minor project.

First, I am truly grateful to **Dr. Nitin Padariya** for their constant support and guidance. Their patience, encouragement, and valuable suggestions helped me stay on the right track and understand the project better.

I also want to thank the **School of Information Technology, Artificial Intelligence and Cybersecurity, Rashtriya Raksha University** for providing the facilities and environment that made this work possible.

My friends and classmates deserve a special mention for being there whenever I needed help, ideas, or motivation.

And finally, I want to thank my family for always believing in me and supporting me in every step of this journey.

This project has taught me a lot, and I'm thankful to everyone who played a part in it.

With Sincere Regards,

Parth Gondaliya

M.Sc in Cybersecurity and Digital Forensics

TABLE OF CONTENTS

DECLARATION.....	1
CERTIFICATE.....	2
ACKNOWLEDGEMENT.....	3
TABLE OF CONTENTS	4
LIST OF FIGURES	8
Abstract.....	12
1. Introduction	13
1.1 Purpose	13
1.2 Introduction to cloud computing	13
1.3 Cloud computing service provider's	14
1.4 Term cloud computing	14
1.5 History of cloud computing	14
2. Background study/ Literature review	17
2.1 Google Drive Forensics by Security Blue Team (2024)	17
2.2 MEGA Cloud Client Forensics (Mishra et al., 2022).....	17
2.3 pCloud Forensic Analysis from a Volatile Memory Perspective (Ahmad & Hamid, 2020)	18
2.4 OneDrive Forensics on Windows Systems (2025).....	18
3. Important components of cloud architecture	19
3.1 Cloud Computing architecture	19
3.1.1 Front end:.....	19
3.1.2 Back end:	20
3.2 Types of cloud computing	20
3.2.1 Public cloud:.....	20
3.2.2 Private cloud:.....	20
3.2.3 Hybrid cloud:.....	20
4. Benefits of cloud computing	21
4.1 Accessibility Anywhere.....	21
4.2 Less Hardware and Software.....	21
4.3 Centralized Security	21
4.4 High Performance and Availability.....	21
4.5 Quick Application Deployment.....	21

4.6	Real-Time Insights	21
4.7	Business Continuity.....	21
4.8	Cost Efficiency	21
4.9	Virtualization.....	22
4.10	Eco-Friendly	22
5.	Cloud storage architecture	23
5.1	Data storage layer:	23
5.2	Data management layer:	24
5.3	Data service layer:	24
5.4	User access layer:	24
6.	Advantages/disadvantage of cloud storage	25
6.1	Advantages of cloud storage	25
6.1.1	Anywhere, Anytime Access	25
6.1.2	Scalability and Flexibility.....	25
6.1.3	Cost Efficiency	25
6.1.4	Ransomware/Malware Protection	25
6.1.5	No Maintenance Required.....	26
6.2	Disadvantages of cloud storage	26
6.2.1	Vulnerability.....	26
6.2.2	Internet Dependency.....	26
6.2.3	Cost.....	26
6.2.4	Issues in Security and Privacy.....	26
7.	Cloud storage forensics	27
8.	Problem statement.....	28
8.1	Digital Forensics in Cloud Computing.....	28
8.2	Developing a Cloud Forensics Strategy	28
8.3	Security and Forensic Issues in Cloud Environments	28
9.	Procedure for digital investigation of cloud storage service.....	29
9.1	Identification:	29
9.2	Preservation:	29
9.3	Collection:	29
9.4	Analysis:	29
9.5	Reporting:	29
10.	Methodology.....	30

10.1 Flow of work	31
11. Tools.....	32
11.1 Autopsy forensic tool	32
11.2 Easy to use	32
11.3 Extensible	32
11.4 Fast	32
11.5 Cost effective.....	33
11.6 FTK Imager 4.7.1.2	33
11.7 Hex editor neo	33
11.8 Wireshark	33
11.9 VMWare	33
11.10 Hindsight	33
12. PCloud storage service	33
12.1 File synchronisation.....	34
12.2 To add a new local folder to the sync:.....	34
12.3 How to upload files through the website	35
12.4 How to upload files through PCloud Drive	36
12.5 How to retrieve your files.....	36
12.6 Ease of use	36
12.7 Security and encryption.....	36
12.8 File versioning	36
12.9 How to use PCloud Transfer	37
12.10 PCloud installation process	37
12.11 RAM dump.....	41
12.12 Disk analyses	41
12.13 Browser data artifact.....	43
13. Mega sync	46
13.1 Installation process	47
13.2 RAM dump.....	49
13.3 Disk analysis.....	53
13.4 Browser artifacts.....	55
13.5 Live browser artefact.....	57
14. One drive	58
14.1 installation process	58

14.2 RAM dump.....	61
14.3 Disk creation.....	64
14.4 Disk analysis.....	65
14.5 Browser artifact	68
14.6 Live browser artifact.....	69
15. Google drive	71
15.1 Introduction to google drive:	71
15.2 Installation	72
15.3 RAM dump.....	77
15.4 Browser side forensic	78
15.5 Disk analysis.....	79
15.6 Live browser artifact.....	81
Findings.....	82
Challenges.....	83
Conclusions.....	84
References	85

LIST OF FIGURES

Figure 1 flow of cloud.....	12
Figure 2 flow of work	13
Figure 3 Time line of cloud History	14
Figure 4 Milestones of cloud History	15
Figure 5 general Cloud Components	18
Figure 6 Work Flow	30
Figure 7 Pcloud Local Drive.....	33
Figure 8 Pcloud listed in the Drive list	33
Figure 9 Pcloud Sync Setting.....	34
Figure 10 Pcloud Backup Folder	36
Figure 11 Pcloud 5 GB space Limited Setting.....	36
Figure 12 Pcloud Disk Extension	37
Figure 13 Pcloud Version	37
Figure 14 Pcloud Encryption Folder.....	37
Figure 15 Pcloud Encryption Folder Setting	38
Figure 16 Pcloud Crypto folder empty in lock	38
Figure 17 Pcloud Encryption folder lock	38
Figure 18 Pcloud crypto folder unlock	39
Figure 19 Pcloud size shown after unlock	39
Figure 20 Rewind state	39
Figure 21 Email Id shown in Ram Dump	40
Figure 22 Crypto Password reveal in Ram Dump	40
Figure 23 Encrypted hand shake	40
Figure 24 Pcloud DB Folder	40
Figure 25 Pcloud DB find used id.....	41
Figure 26 Pcloud DB Table	41
Figure 27 List of all Folder sync with Pcloud.....	41
Figure 28 Pcloud Files Sync List	42
Figure 29 Pcloud Hidden Folder.....	42
Figure 30 Total Browser History Found	42
Figure 31 Browser History email verify for Pcloud Service	43
Figure 32 Cache Preview of crypto folder.....	43
Figure 33 Pcloud Version	43

Figure 34 Pcloud Login data.....	44
Figure 35 Report created by the Autopsy	44
Figure 36 Extention installed.....	44
Figure 37 Login history with email id and time-stamp.....	44
Figure 38 Mega setup Installation.....	46
Figure 39 Sync Setting.....	46
Figure 40 Sync folder selection	46
Figure 41 Complete Setup	47
Figure 42 No Local Disk.....	47
Figure 43 Sync Folder Setting	47
Figure 44 Email id Found	48
Figure 45 Password not found	48
Figure 46 Log Files.....	48
Figure 47 Sync DB.....	49
Figure 48 List of files are Synced in Cloud	49
Figure 49 Browser view of cloud.....	50
Figure 50 Files deleted from cloud effect the PC	50
Figure 51 Same effect on browser	50
Figure 52 Restore files from the cloud recycle	50
Figure 53 New file is created in the Folder.....	51
Figure 54 Encrypted file sync	51
Figure 55 Encrypted hand shake	51
Figure 56 Cloud Recovery key	52
Figure 57 Book Mark the key	52
Figure 58 Deleted file and sync file list	52
Figure 59 Confirmed use of the Mega cloud	52
Figure 60 Mega sync folder	53
Figure 61 Mega version file.....	53
Figure 62 Log files.....	53
Figure 63 Successfully installed cloud program.....	53
Figure 64 All file converted in .lnk which are synced.....	54
Figure 65 Browser history	54
Figure 66 Mega cloud .exe.....	54
Figure 67 Autopsy themself create cloud storage separated.....	54
Figure 68 mega login details.....	54

Figure 69 Recent activity of login mega cloud	55
Figure 70 Login DATA files.....	55
Figure 71 Report make from autopsy successfully	55
Figure 72 hindsight browser history by timeline	56
Figure 73 hindsight browser history find.....	56
Figure 74 installation steps	57
Figure 75 successfully installed	57
Figure 76 Personal vault setup	58
Figure 77 Personal vault setup	58
Figure 78 Sync folder list.....	59
Figure 79 sync status.....	59
Figure 80 Sync and backup folder setting.....	59
Figure 81 Version of the one drive	60
Figure 82 User id Reveal Ram Dump.....	60
Figure 83 Sync File Location reveal in ram dump	61
Figure 84 Encrypted hand shake.....	61
Figure 85 Log Files	61
Figure 86 Log File show in plain text.....	62
Figure 87 SyncDiagnostics.log for track all thinks.....	62
Figure 88 Device health summary track	63
Figure 89 image creation	63
Figure 90 successfully created image	63
Figure 91 all files in .lnk	64
Figure 92 .ink file location.....	64
Figure 93 list of all files are in cloud	64
Figure 94 all deleted and move files	65
Figure 95 Real Desktop image.....	65
Figure 96 Found OCSI.db file	65
Figure 97 Found PDF file as image	66
Figure 98 screenshots found	66
Figure 99 files are deleted.....	67
Figure 100 browser history	67
Figure 101 Screenshots data found	67
Figure 102 Email ID found profile	68
Figure 103 created successfully report	68

Figure 104 histroy of one drive login	68
Figure 105 onedrive login id.....	69
Figure 106 onedrive local and session storage	69
Figure 107 Gdrive login page	71
Figure 108 Gdrive successfully installed	71
Figure 109 Gdrive installed path.....	72
Figure 110 Gdrive DB files.....	72
Figure 111 Gdrive User Data files	73
Figure 112 Gdrive User Data files	74
Figure 113 Gdrive local Disk.....	74
Figure 114 List of DB files created by Drive	74
Figure 115 Sync Data entry DB file	75
Figure 116 Data Entry Details with Epoch Time.....	75
Figure 117 Sync DB entry	75
Figure 118 File Sync Epoch Time	76
Figure 119 Ram Dump through Task Manager	76
Figure 120 Ram Dump Files.....	76
Figure 121 File Location Reveal at Sync Time	76
Figure 122 Dump File Created	77
Figure 123 Dump File Stored in Temp Folder.....	77
Figure 124 Email Id found in Ram Dump	77
Figure 125 Find GDrive location.....	78
Figure 126 Gdrive installed .exe	78
Figure 127 Autopsy Suggested Cloud installed in this user	78
Figure 128 Browser history	78
Figure 129 Sync DB.....	78
Figure 130 uploaded successfully document are in lnk	79
Figure 131 GDrive DB we can't find the Last sync	79
Figure 132 Experiment. DB	79
Figure 133 Root-Preference.DB	79
Figure 134 Google Drive report created successfully.....	80
Figure 135 finding a history with auto fill data	80
Figure 136 Local and session storage	80
Figure 137 email id used to search and profile name	80

Abstract

Cloud Storage Forensics

Submitted By

Gondaliya Parth Vinodbhai

Supervised By

Dr, Nitin Padariya

Cloud storage services such as PCloud, MEGA, OneDrive, and Google Drive are now widely used for storing and sharing data. However, as these platforms grow, they also create new challenges for digital forensic investigators, especially because the actual data is stored on remote servers that cannot be accessed directly. This project explores how much useful forensic evidence can be recovered from a user's device when cloud storage services are used.

To study this, different user actions—like uploading, downloading, deleting, and syncing files—were performed on multiple cloud services. Tools such as Autopsy, FTK Imager, Hex Editor Neo, Hindsight, Wireshark, and VMware were used to examine both the disk and RAM for traces of activity. The analysis showed that even though cloud systems keep their internal data hidden, a significant amount of evidence remains on the user's computer. This includes log files, database entries, browser histories, cached information, user IDs, and sometimes even sensitive details found in RAM.

The results highlight the differences between cloud providers: some focus strongly on security and encryption, while others leave behind more detailed local artifacts that help investigators. The study also reflects on the difficulties faced during cloud investigations, such as encrypted data, fast-changing environments, and legal restrictions across countries.

Overall, this project provides a practical understanding of how cloud storage forensics works and offers a clear methodology for identifying and analyzing client-side evidence. These findings can help forensic investigators better handle cases involving cloud-based data.

1. Introduction

1.1 Purpose

The rapid growth and improvement of cloud technology is taking digital forensics to a whole new level. The main goal of this project was to investigate cloud storage and understand how files can be examined—whether they still exist or have been deleted. Our analysis shows that several artifacts remain even after files are erased from cloud storage. We also found that the number and type of artifacts change depending on actions such as creating, deleting, uploading, transferring, or moving files within the application.

1.2 Introduction of cloud computing

Cloud computing and cloud forensics are two closely related fields that have evolved together over the past few decades.

Cloud Computing is referred to as accessing and storing data and providing services related to computing over the internet. It simply refers to remote services on the internet manage and access data online rather than any local drives. The data can be anything like images, videos, audios, documents, files etc.

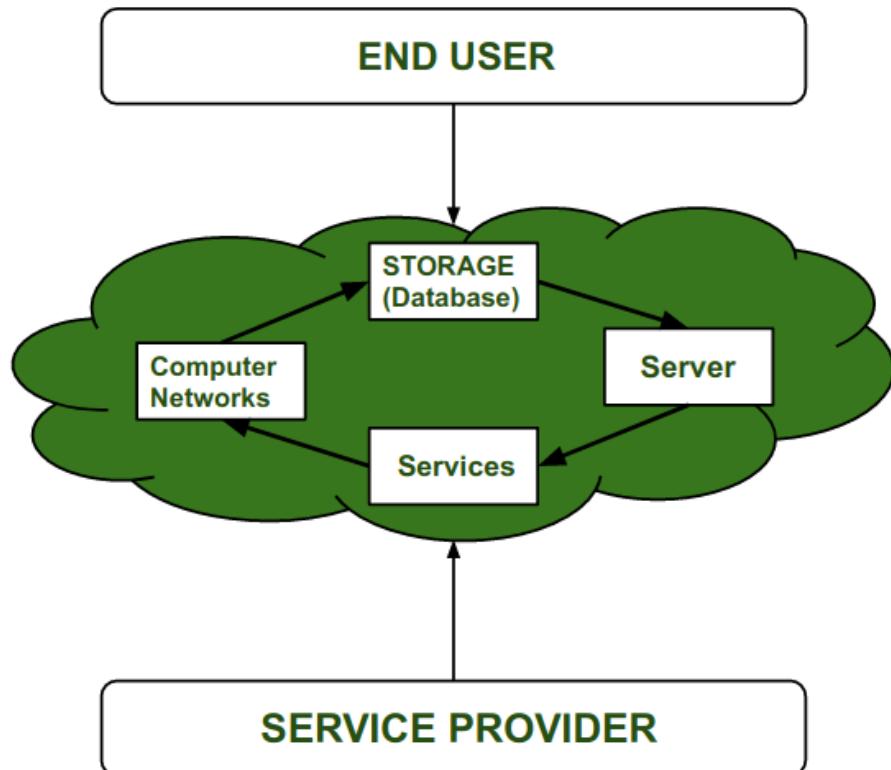


Figure 1 : flow of cloud

1.3 Cloud service provider's

Cloud computing is in high demand, and many major organizations now provide cloud services. Some of the leading cloud service providers like Amazon AWS, Microsoft Azure, Google Cloud, and Alibaba Cloud.

1.4 Term cloud computing

The term "cloud computing" was coined to describe the concept of delivering computing services on the internet, without the need for on-premise hardware and infrastructure. The word "cloud" was used as a metaphor for the internet, which is often represented as a cloud in network diagrams.

The idea behind cloud computing is that computing resources, such as processing power, storage, and applications are made available also to users over the internet, much like electricity is provided through power grids. Users can access these resources on-demand and pay only for what they use, rather than investing in expensive hardware and infrastructure that may sit idle for long periods of time.

The term "cloud" also reflects the idea that the underlying hardware and infrastructure are abstracted away from the user, who only sees the services and applications that are made available through the cloud platform. This abstraction allows cloud providers to manage the underlying infrastructure more efficiently, while also providing greater flexibility and scalability to users.

1.5 History of cloud computing

Before modern computing evolved, systems relied on a client-server architecture where all data and control were stored on the server side. If a user wanted to access any information, they first had to connect to the server and then receive the necessary permissions. However, this model had several disadvantages. To overcome those issues, distributed computing was introduced. In this approach, multiple computers were connected through a network, allowing users to share resources whenever required. Although distributed computing improved flexibility, it still came with certain limitations.

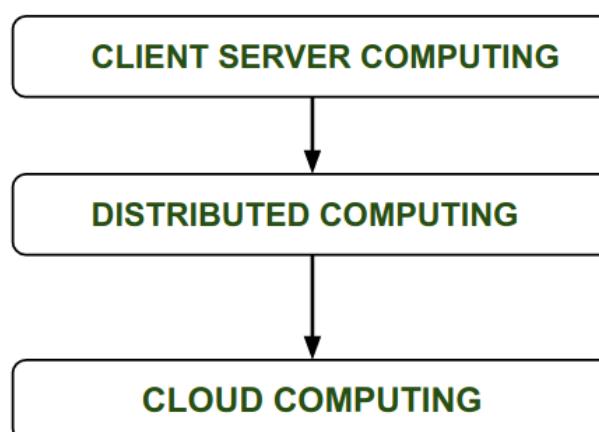


Figure 2 : flow of Work

"Computing may someday be sold as a utility, just like water and electricity," said John McCarthy in a 1961 speech at MIT. Although it was a visionary idea, people were not prepared to embrace it at the time. The concept didn't get much attention, and not much research was done on it because they thought the technology already in place was adequate for their needs. But as technology advanced, McCarthy's concept started to become more well-known. The idea was eventually implemented after a number of years. In 1999, Salesforce.com was among the first to successfully implement it, signaling the start of contemporary cloud computing services.

- When businesses began distributing enterprise apps online, it signaled the beginning of a significant change in the way software and services were offered, which in turn led to the rise of cloud computing.
- **2002:** Amazon launched Amazon Web Services (AWS), which provided computing power and online storage.
- **2006:** Google Docs, which enables users to create and share documents directly through the cloud, was introduced by Google in 2006.
- **2006:** Amazon formally extended AWS, offering businesses all over the world scalable, adaptable, and reasonably priced cloud solutions.
- **2007:** The launch of Dropbox, a file-hosting service that provided simple file synchronization and storage, developed by an MIT student.

Cloud Computing History

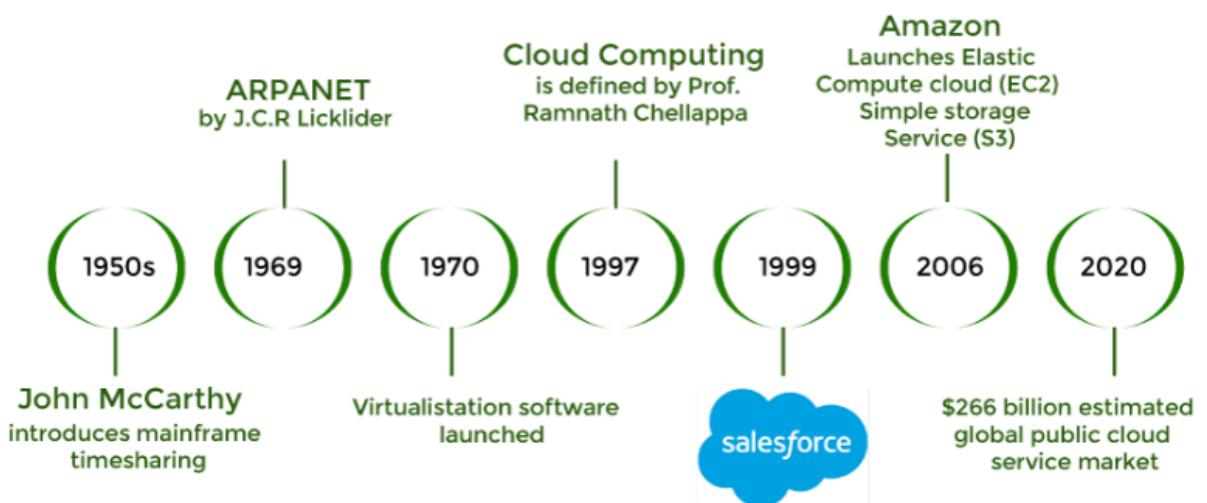


Figure 3 : Time line of cloud History

- **2008:** Google made App Engine generally available, which allowed developers to create and deploy applications without managing the underlying infrastructure.
- **2010:** Market entry in the cloud by Microsoft, named Azure, offering services much like AWS, was focused strongly on enterprise-level solutions.

- **2012:** Google launched Google Drive, enabling people or enterprises to store, share, and collaborate on files in the cloud.
- **2015:** Multi-cloud solutions became a strategic approach for many organizations to address performance, reliability, and cost efficiency by using several cloud providers.
- **2020:** Cloud computing began to focus more on security, adding more advanced capabilities such as AI, machine learning, and automation to make cloud platforms more powerful and intelligent.
- **2023:** The integration of advanced AI models, including OpenAI's GPT-4 with cloud platforms, increased the possibilities of AI in business, research, and realworld applications.

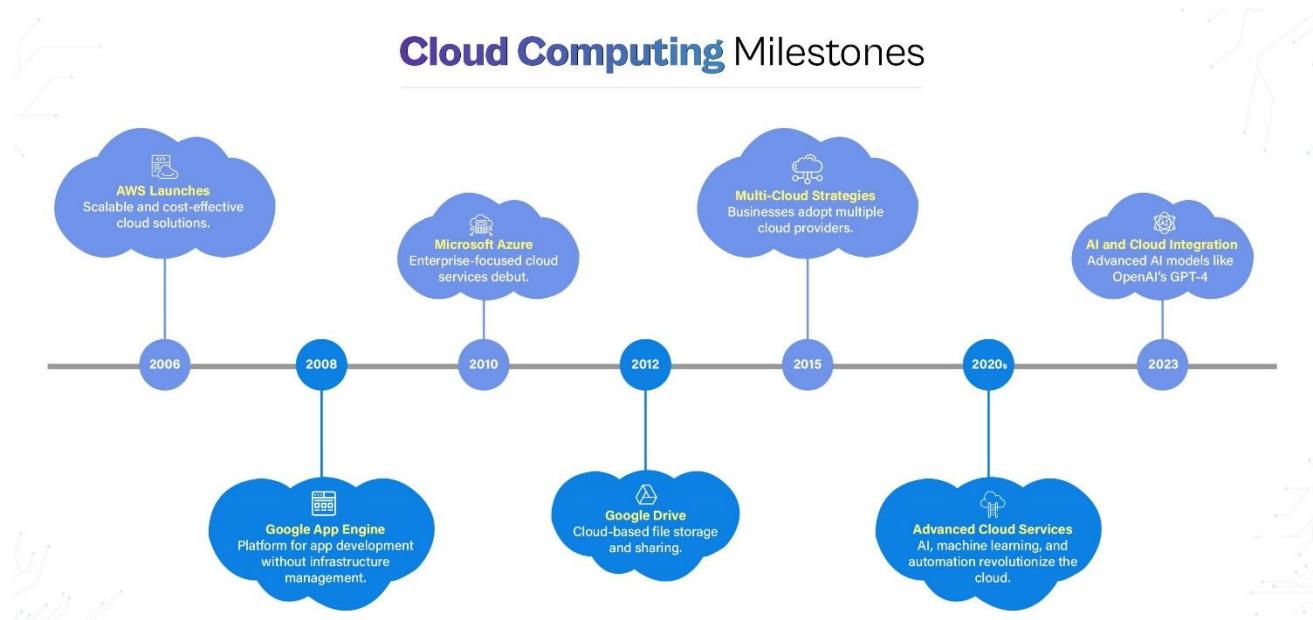


Figure 4 : Milestones of cloud History

2. Background study/ Literature review

2.1 Google Drive Forensics by Security Blue Team (2024)

This paper analyses the Google Drive desktop application's leftovers from a forensic point of view on Windows OS. The author points that regular activities—like uploading, deleting, or syncing files—will result in the registry keys, log folders, and some SQLite databases used by the DriveFS service being updated. Even if a cloud user deletes files, sometimes metadata and activity entries are left on the device which allows the detective to re-create the timeline of file interactions. The paper also emphasizes the importance of memory analysis and states that the running Drive processes store temporary information in RAM, which can be used to disclose filenames or session activity. To sum up, it shows that Google Drive has a huge variety of artefacts at the endpoint level that can accurately be used to revive user actions during a forensic examination.

2.2 MEGA Cloud Client Forensics (Mishra et al., 2022)

This study provides a detailed examination of the MEGA cloud client on Windows and Android devices. The authors conduct controlled user operations such as uploading, downloading, and sharing to spot a great variety of artefacts that include cached metadata, recent file lists, logs, and timestamps. The traces left on the device are very useful for user activity reconstruction since they persist even after the content has been deleted from the cloud. On Android, the investigation points to the application-specific folders and preference files that contain the user activity records, whereas the Windows platform holds the MEGA logs, configuration files, and registry entries. The researchers say that the MEGA service is reliable when it comes to leaving behind forensic traces that can help researchers investigating the use of cloud storage on different platforms.

2.3 pCloud Forensic Analysis from a Volatile Memory Perspective (Ahmad & Hamid, 2020)

This paper highlights the generally neglected domain of volatile-memory forensics when investigating cloud storage. The researchers demonstrate, by analyzing RAM after various actions such as uploading and downloading files using the pCloud client, that memory contains some very important temporary artifacts. These include session tokens, API references, partial filenames, and metadata related to recent user activities. Because such artifacts do not always show up in disk-based logs or databases and may be lost after the system is shut down, the authors stress the importance of live-memory acquisition in investigations dealing with cloud applications. These findings do indeed reinforce the view that RAM forms a very important source of evidence, particularly in modern cloud clients relying on encrypted or transient processes.

2.4 OneDrive Forensics on Windows Systems (2025)

This most recent research covers how the OneDrive desktop client stores information about user activity on Windows devices. Key registry entries, as found by the authors, hold account information, synced folder locations, and unique cloud identifiers, all aiding to confirm user profiles and access paths. They also analysed OneDrive's core database, SyncEngineDatabase.db, which tracks local file interactions with cloud-only items that have never been fully downloaded. In addition, their research reviewed OneDrive log files stored on the user profile, illustrating how file upload, download, rename, and deletion events are recorded over time. Collectively, these artefacts paint a clear picture of user behaviour, underscoring OneDrive as a strong source for client-side evidence in cloud-storage forensic investigations.

3. Important components of cloud architecture

3.1 Cloud Computing architecture

Cloud computing architecture is made up of several loosely connected components. Overall, it can be broadly divided into two main parts:

1. Front ends
2. Back ends

Each of these components is connected through a network, typically the internet. The diagram below provides a visual representation of the overall cloud computing architecture:

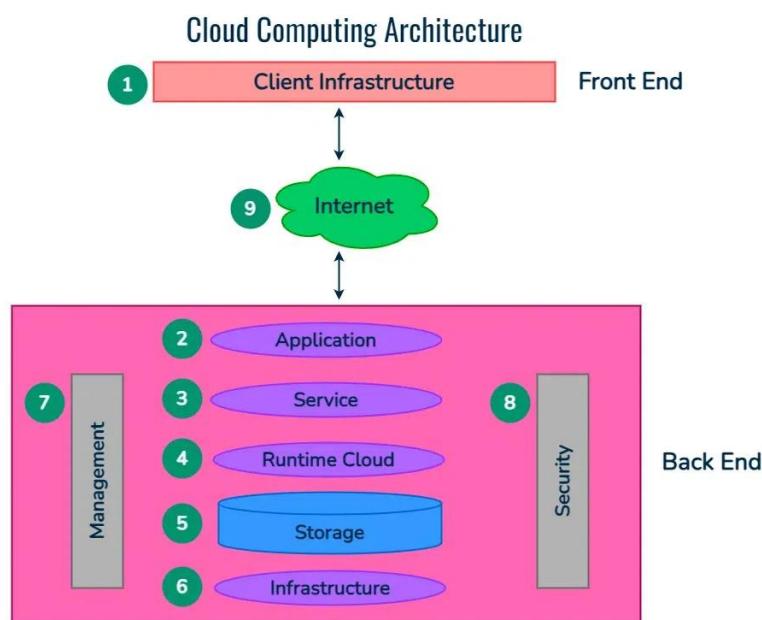


Figure 5 : general Cloud Components

Cloud computing architecture encompasses several critical building blocks. Among them are the client-side infrastructure, applications, services, runtime environments, data storage systems, management tools, and security mechanisms. All the components mentioned above collectively create a complete cloud computing architecture.

3.1.1 Front end:

The client interacts with the cloud through the front end side, which includes the user interface and the client-side application. Both of these are essential for accessing any cloud platform. The front end typically consists of web browsers for ex. Chrome, Firefox, or Opera, as well as client applications and mobile devices.

3.1.2 Back end:

The backend is responsible for managing all the resources needed to deliver cloud computing services. It includes components such as security systems, large-scale data storage, servers, virtual machines, and traffic management tools. Together, these elements ensure that the cloud operates smoothly, securely, and efficiently.

3.2 Types of cloud computing

There are different types of ways cloud technology is implemented. The model is determined for you to base on a thorough assessment of the operations of the business. The best solution is the one that meets your outmost needs there are three different ways to deploy cloud services on a Public cloud, Private cloud and Hybrid cloud.

3.2.1 Public cloud:

The third-party cloud service provider owns and runs the business of providing cloud compute resources such as servers, software, storage, hardware all over the internet. A typical example of a public Cloud is Azure from Microsoft All hardware, software and auxiliary system are owned and run by the cloud service provider. The public cloud service is delivered to users via a web browser

3.2.2 Private cloud:

The Private cloud is operated in the same manner as the public except for the resource of the Private cloud is used by one organization. The infrastructure could be located on the company's premises or may be outsourced to a third-party business to host on behalf of the organization. This means the service is run on a private network

3.2.3 Hybrid cloud:

The Hybrid cloud model is a merger of the public and private clouds making it possible to share computing resources between the 2 architecture, a good implementation of the hybrid cloud provides higher elasticity to the company. This because the business has many options in deployment which best for the effective and efficient use of the organization's existing resources.

4. Benefits of cloud computing

4.1 Accessibility Anywhere

Cloud computing allows employees, clients, and customers to access data from any device and location. Everyone stays updated whether they're in the office or on the go.

4.2 Less Hardware and Software

You won't have to purchase or look after any server, cables, or routers. The cloud service takes care of everything and charges a monthly fee, which reduces the overall cost of a business.

4.3 Centralized Security

Data is stored in the provider's data centers, where it is securely backed up. Using encryption and two factor authentication are among the features that provide better protection against data loss or breaches.

4.4 High Performance and Availability

Cloud infrastructure offers quick performance and almost no downtime at all. The providers are the ones who take care of the updates and fixes automatically thus allowing the users to enjoy their uninterrupted operations.

4.5 Quick Application Deployment

Applications can be deployed immediately within the same time frame of waiting for hardware installation. This benefits the process of business changes and the ability to scale up or down flexibly.

4.6 Real-Time Insights

Cloud platforms provide instant access to relevant data, in turn helping businesses to make smarter and faster decisions by interpreting information in real-time.

4.7 Business Continuity

During a catastrophe, the safe keeping of data and systems is achieved thanks to remote backups ensuring continuation of business operations.

4.8 Cost Efficiency

Though an initial investment is required, the maintenance costs that are normally associated with on-premises servers are eliminated by cloud computing, thus making it a long term money saver. The flexibility is provided by the pay-as-you-go pricing model.

4.9 Virtualization

An auto-scaling property makes it convenient to scale up or down just as easier to avoid maintenance, overhead, and human verifications that are changes in the operating environment.

4.10 Eco-Friendly

The implementation of cloud computing in the IT industry results in a considerable reduction of energy consumption as well as carbon footprint, which is up to 90%, thus it is considered a more environment-friendly and sustainable IT solution.

5. Cloud storage architecture

Cloud storage different from traditional storage. Operationally, cloud storage is designed and deliver a wide range of online cloud storage services, while conventional storage systems is mainly built for high-performance computing and transaction processes. Performance-wise, emphasis in cloud storage lies in data security, reliability, and efficiency. Serving a greater number of users, offering more comprehensive services, and running in a more complex and ever changing network environment, cloud storage is faced with much greater technological challenges than traditional storage in providing high-quality services.

Cloud storage systems support not only access to traditional files, such as those based on the POSIX standard, but also manage large-scale data and provide public service function, maintaining data in background from data management perspective.

Commonly, cloud storage is divided into four layers, which are the data storage layer, data management layer, data service layer, and the user access layer. Figure 1 shows the cloud storage architecture as proposed by Zhou Ke et al. (2010).

5.1 Data storage layer:

The cloud storage system provides various storage services, and all the data stored within forms a huge shared pool. This must be appropriately structured and managed so that efficient storing and fast access are ensured. Traditional methods of data organization rely on a single server, which cannot handle the high throughput and large storage demands of multiple users across a wide-area network.

While peer-to-peer storage systems improve performance, they entail a very large number of nodes and complex coding techniques in order to maintain data reliability. Organizing data using different cloud storage services is far more suitable for modern online storage needs.

Cloud storage relies on data centers distributed across different regions. Geographical dispersal enables the system to provide services of high quality for a big number of users located in diversely spread areas. The storage layer manages enormous amounts of data in a unified manner by interconnecting various types of storage devices. It also allows centralized management, real-time monitoring, and dynamic expansion of storage capacity at any time.

Overall, cloud storage systems work as service-oriented, distributed storage environments that can handle large-scale, reliable, and flexible data storage.

5.2 Data management layer:

The Data Management layer provide a public management interface to the upper layers for each kind of cloud service. The key functionalities include user management, security management, replica management, and policy or strategy management. In this way, it works like a bridge that connects seamlessly the applications of the upper level with the lower-level storage services.

In addition, it lets different storage devices cooperate, enabling them to provide a broader range of services and better performance.

5.3 Data service layer:

This layer interacts directly with the user and is the most flexible part of the system. Depending on the user's needs, different application interfaces can developed to provide services such as data storage, public resource access, multi-user data sharing, or data backup.

5.4 User access layer:

This layer allows authorized users to log in to the cloud storage platform from any location through a standard public interface, giving them seamless access to their stored data.

6. Advantages/disadvantage of cloud storage

6.1 Advantages of cloud storage

The main advantage of these services as Google Drive, Apple I Cloud, Mega Drive, and Microsoft OneDrive to users is their data is stored in a virtual location in the cloud while a local version exists on their computer system or smartphone. Its synchronization with the cloud does not require any user interaction after the installation of the Client Application. This means there always an offline version of the data stored locally for easy access while the backup is in the cloud and updates any time there is internet connectivity.

6.1.1 Anywhere, Anytime Access

No matter where you are, you can log in to your files with just an internet connection. This global accessibility supports remote work and collaboration, allowing employees to co-edit documents in real-time (e.g. Google Drive, Microsoft 365).

6.1.2 Scalability and Flexibility

Need an extra 10TB for a seasonal campaign? Scale up instantly. Experiencing a quiet quarter? Scale back down. Cloud providers' pay-as-you-go or tiered pricing models make it easy to adapt to business fluctuations.

6.1.3 Cost Efficiency

Cloud storage reduces or eliminates:

- Server infrastructure costs
- Physical storage facility expenses
- Specialist staff overheads
- You pay for what you use, avoiding under- or over-investment.

6.1.4 Ransomware/Malware Protection

Ransomware is one of the most dangerous types of malware, and unfortunately, it appears in the news far too often. One of the scariest things about ransomware is that it doesn't just infect the local computer it also searches the entire network for shared folders and files to encrypt.

The good news is that cloud storage can help protect your data. Since cloud platforms require proper authentication and maintain secure backups, it becomes much harder for ransomware or other malware to access, encrypt, or destroy your files. This added layer of protection can be a major advantage during an attack.

6.1.5 No Maintenance Required

With cloud storage, your subscription fee helps cover the company's costs for maintaining and upgrading its servers.

6.2 Disadvantages of cloud storage

6.2.1 Vulnerability

Most PCs and servers that store data depend on an internet connection. Since cloud solutions are naturally internet-based, they are constantly connected to other computers and servers. This connectivity, while essential, also makes the vulnerable to attacks from malicious users on the network.

6.2.2 Internet Dependency

An internet connection is a key resource for cloud storage. It was a significant disadvantage in the past but this isn't the case any more since the internet has blended into our daily life to such a great extent. Offline file storage and later retrieval is allowed but the internet must be there all the time when the system wants to carry out updating or syncing of the data.

6.2.3 Cost

Even though cloud storage is usually a cheap option, it can still not be used for short-term or very small-scale projects depending on the pricing structure of the provider. Sometimes, consumers get trapped in lengthy agreements. To illustrate, when a user needs storage for only six months but the provider requires a minimum two-year subscription, the user ends up paying for an extra 18 months, which is not a sensible financial decision.

6.2.4 Issues in Security and Privacy

Concerns about security and privacy are among the major drawbacks of cloud storage. Storing confidential data in the cloud requires handing it over to a third-party provider, which means users must place a high level of trust in the cloud vendor. This dependency can create uncertainty, especially when handling sensitive or critical information.

7. Cloud storage forensics

Digital forensic is defined as the process of gathering and analysing electronic evidence for legal purposes, criminal investigation or civil dispute.

It's difficult to make a case legally when it has to do with cloud computing as the digital forensic analyst has to acquire and analyse the electronic evidence adhering to the same standards as with traditional server-based system. This is not easy as the Investigator will have to establish the exact cloud service provider and identify the user details and password for the cloud storage account. Such details can be retrieved by taking a forensic image of the computer/Mobile Device for analysis.

These type of Cloud services are also referred to as Synchronization services. This means that as the user stores the information on a digital device is synchronized, a copy of the data is saved in remote server Spread across several locations of data center.

With the rate of growth cloud service there is a high likelihood of such crimes occurrence - A criminal could leak confidential information of companies stored in a cloud storage service by hacking a cloud service that allows account holders to store documents and images access them everywhere with any digital device.

An example if an investigator in Ghana identifies a suspect has stored data with a cloud storage service in the USA. The process of gaining access and securing the data relies on agreements and MOUs across those countries with valued legal systems. This process to get legal authorization may take longer to achieve due to several reasons. While this is happening the suspect may continue to have access to an account and compromise the evidence.

One of the difficult parts of an investigation in cloud storage service is the challenge to find which user credential did from the time of subscription to the service till the completion of the service term.

Once the authorization and authentication to the cloud storage account is made the forensic investigator can begin legal process with the service provider to protect the data under investigation. The process can bring challenges especially when the data center of the cloud storage service provider is located in a different jurisdiction to where the crime was committed. This call for collaboration and cooperation's among law enforcement agencies.

Computer system users create documents, images, emails and surf the internet. These activities leave traces on the computer which are good sources of digital evidence. The actual files may not reside on the local machine and such the forensic expert may rely on artifacts left behind on the system to trace user activities. The logs recorded by the cloud service provider can provide audit trails of user activities, this information is however kept private and protected by the cloud storage service provider.

8. Problem statement

8.1 Digital Forensics in Cloud Computing

As a result of this rapid adoption of cloud computing, organizations and individuals increasingly store and manage their data on online platforms. This increasing reliance has opened new challenges for forensic investigators because, during conventional investigations, forensic experts had access to these physical devices from which they could gather and analyze evidence. In cloud environment, investigators rarely have such access because the data is distributed over several servers owned and managed by third-party providers, which makes tracing user activities difficult, preservation of digital evidence, or ensuring its integrity challenging.

The key challenge is, therefore, to acquire, preserve, and verify digital evidence from cloud storage systems where one does not have control the physical infrastructure or the exact location of the data.

8.2 Developing a Cloud Forensics Strategy

Today's organizations are under stringent legal and regulatory imperatives to manage what digital information is stored, retained, and discarded. When digital data is stored in the cloud, it often resides in multiple countries and is subject to a variety of privacy and data-protection laws. Issues of ownership, retention time, and privacy rights of users may be unclear.

Consequently, there is an increasing demand for the development of a cloud forensics strategy that supports the legality of evidence collection and preservation, respects users' privacy, and adheres to international data regulations. It should also allow organizations to ensure compliance with existing laws and to prepare for forensic investigations if incidents occur.

8.3 Security and Forensic Issues in Cloud Environments

Cloud computing presents many different security and forensic issues. The transient nature of the cloud ensures that user activities, virtual machines, and data flows can change quickly, with the result that it becomes difficult to find out who performed a certain action and accessed given information. In a shared multi-tenant environment, tracing back malicious activity to a specific user or system may pose an especially challenging issue.

Additionally, replication, migration, and synchronization of data by cloud services can affect the nature of the digital evidence; this raises concerns about how cloud storage evidence can retain its integrity and credibility when presented for investigation. The problem gets even more complex when presenting findings in court, since examiners must prove that evidence has not been modified in any way throughout an investigation.

9. Procedure for digital investigation of cloud storage service

There are many forensic investigation models proposed. There is a common one that is accepted and seen as standard in digital forensics practice. They are 5 stages process

- Identification of the Electronic Evidence
- Preservation of Electronic Evidence
- Collection of Evidence
- Analysis of Electronic Evidence
- Reporting

9.1 Identification:

The first stage is to find the potential sources of information that will be relevant to the investigation. The search may start from known to unknown areas. Smartphones, Computers and other digital devices.

9.2 Preservation:

This step is very important as the digital evidence needs to be preserved by protecting the crime scene and taking shots/pictures of all items in the surroundings. Proper documentation needs to be taken of all items identified at the scene. Chain of custody is adhered to at all times.

9.3 Collection:

Gathering electronic information which may be important to the investigation. Collection may involve removing the electronic devices from the scene of the crime and taking then creating a bit-by-bit copy of it, or printing. Whichever way the evidence is collected care must be taken not to compromise the integrity of it.

9.4 Analysis:

Using various forensic techniques and tools the evidence is subject to forensics analysis or examination and any lead relevant to the investigation is recorded. A conclusion may be drawn based results of the analysis conducted by the investigator.

9.5 Reporting:

Accurate records are taken through the investigation process. This record may verify when need be, at the court of law. The investigator only report evidence related to the Crime and no other activity.

10. Methodology

This study is experimental in nature and involves a practical demonstration of the identification, collection, preservation, analysis, and presentation of digital evidence. The experiment was conducted using four cloud storage services: Google Drive, OneDrive, MEGA Sync, and pCloud.

To perform the analysis, two types of user activities were examined:

- Browser interactions
- Client application interactions

Across these cloud platforms, the following actions were tested using both the desktop client applications and web browsers:

- File download
- File upload
- File deletion
- File sharing

Since access to the internal data centers of cloud service providers is not available for forensic purposes, this investigation relies on evidence of past data possession found on the user's computer system, as suggested by Sham Zawoad et al. (2012).

10.1 Flow of work

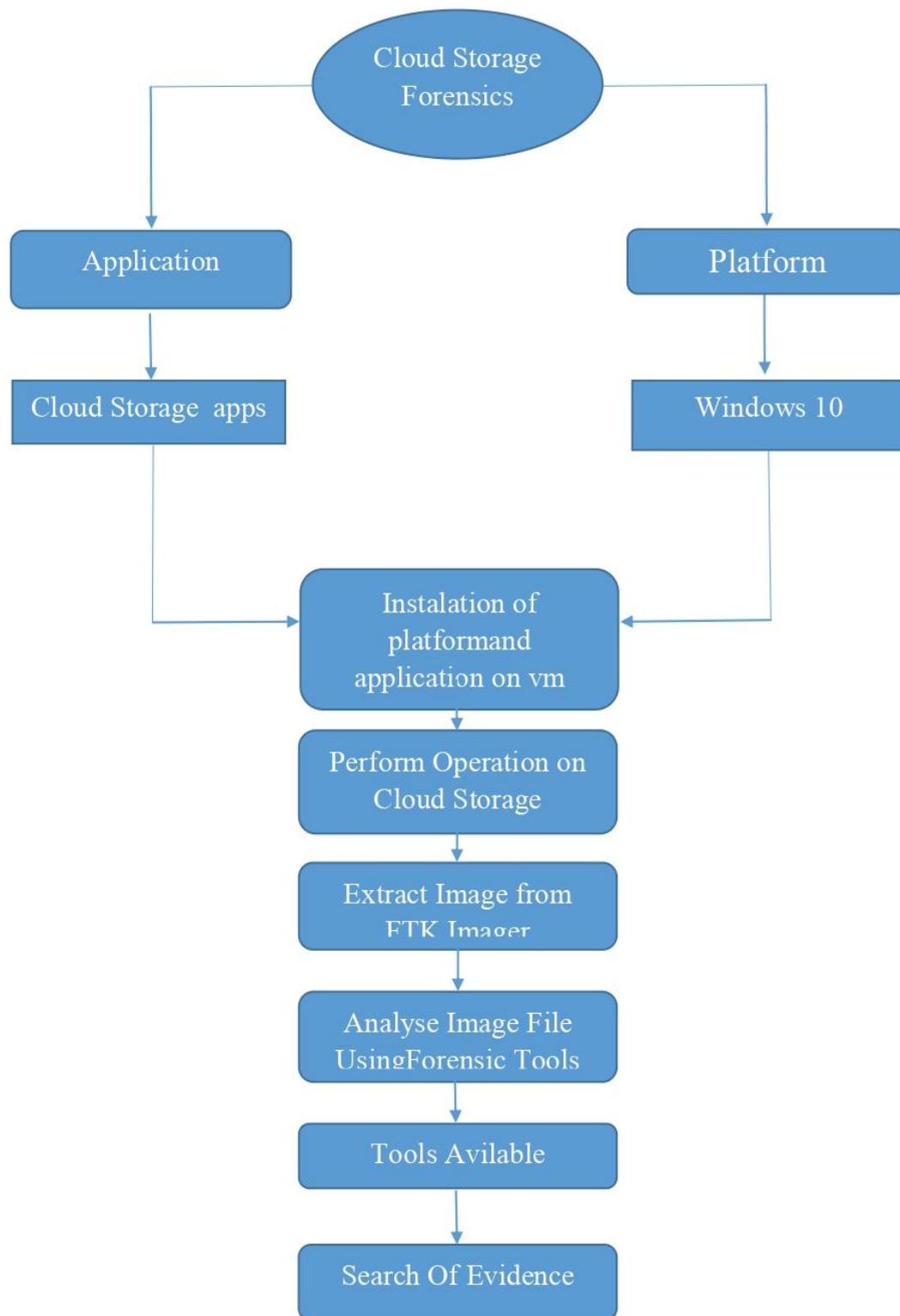


Figure 6 : Work Flow

11. Tools

11.1 Autopsy forensic tool

Autopsy is a digital forensics platform that provides a graphical interface for The Sleuth Kit and other forensic utilities. It is widely used by law enforcement, military investigators, and corporate examiners to analyze digital evidence and determine what activities took place on a computer system. Autopsy can also be used for simple tasks such as recovering deleted photos from a camera's memory card, making it a versatile tool for both professional and personal investigations.

11.2 Easy to use

Autopsy is easy to use, with simple installation and step-by-step wizards. All investigation results are organized in a single, easy-to-navigate tree.

11.3 Extensible

Autopsy is built as an end-to-end platform, offering built-in modules as well as third-party add-ons. These modules provide various forensic functions such as data carving, timeline analysis, keyword search, and file recovery.

- **Timeline Analysis:** Provides an advance graphical interface to view events.
- **Hash Filter:** Identifies known malicious files and ignores known safe ones.
- **Keyword Search:** Uses index search to quickly find files containing specific terms.
- **Web Artifacts:** Extracts browser history, bookmarks, and cookies from Firefox, Chrome, and Internet Explorer.
- **Data Carving:** Recovers deleted files from unallocated space using PhotoRec.
- **Multimedia Analysis:** Extracts EXIF data from photos and allows viewing of videos.
- **Indicators of Compromise:** Scans the system for threats using STIX-based intelligence.

11.4 Fast

Autopsy employs a multi-core setup to perform background tasks in parallel and delivers results to the user immediately upon discovery. It might take several hours for a complete drive search, but you will be informed within minutes if your keywords were found in the user's home directory. For more detailed information refer to the fast results page.

11.5 Cost effective

Autopsy is totally free and open source tool. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools, such as web artifact analysis and registry analysis that other commercial tools do not provide.

Product Version: Autopsy 4.21.0

Sleuth Kit Version 4.12.1

11.6 FTK Imager 4.7.1.2

FTK Imager is a forensic imaging tool from AccessData that creates full or segmented disk images, verifies them with MD5 hashes, and can also mount drives and recover deleted files.

11.7 Hex editor neo

Free Hex Editor Neo is the fastest and large files optimized binary file editor for Windows platform developed by HHD Software Ltd. It's distributed under Freemium model and provides you with all basic editing features for free.

11.8 Wireshark

Wireshark is an open source tool for capture and analysing network traffic and packets. Such a tool is often referred to as a network analyser, network protocol analyser or sniffer.

11.9 VMWare

VMware Tools is an important add-on for virtual machines that helps everything run more smoothly. It installs better drivers, improves system performance, and allows the guest operating system to work more naturally and efficiently with the VMware platform.

11.10 Hindsight

Hindsight is a free tool used to analyze web browser artifacts. It supports Chrome and other Chromium-based browsers and can extract data like history, downloads, bookmarks, cookies, autofill, and more. It then correlates this information and presents it in a timeline.

12. PCloud storage service

pCloud is a widely used cloud storage service known for offering excellent security along with unlimited upload and download speeds. Launched in 2013, it has grown by learning from both the successes and shortcomings of competing services. It is also one of the first cloud storage providers to introduce lifetime subscription plans.

With pCloud, there are no limits on file size or download speed. It has strong security features along with trustworthy backup options. Similar to other cloud storage services like Google Drive and Dropbox, pCloud also allows you to back up your social accounts (such as Instagram, Facebook, and Picasa) as well as your WordPress websites.

You can even mark files as “favorites” to access them offline.

12.1 File synchronisation

The pCloud app and web interface offer several file-sharing options, allowing you to send files and folders wherever you need. Its virtual drive feature also expands your computer’s storage, and any files you upload to that drive can be accessed from any device, anytime, and anywhere.



Figure 7 : PCloud Local Drive

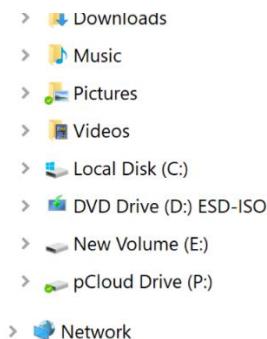


Figure 8 : PCloud listed in the Drive list

You can open your pCloud Drive in your file manager by simply left-clicking or right-clicking the pCloud icon. If you have a Crypto subscription, you can access your Crypto folder and add new folders to your Sync list. You can also use the menu to check your account status and view notifications.

12.2 To add a new local folder to the sync:

- Open the pCloud panel and go to Sync.
- Click Add New and select the local folder.
- Browse to the folder you want to sync.
- Choose the destination folder on your pCloud Drive.
- Select where the folder should sync in your pCloud directory.
- Click Save, then Add Sync.

The sync will begin immediately and the synced folders will be accessible from all devices linked to your pCloud account. You can create multiple sync folders as long as you have enough storage space. If you want your synced folders to be available offline, simply right-click the folder and select “Offline Access (Sync).”

You can choose either the pCloud Drive folder or a local folder for offline access. After making your selection, click “Save” to confirm and complete the synchronization setup.

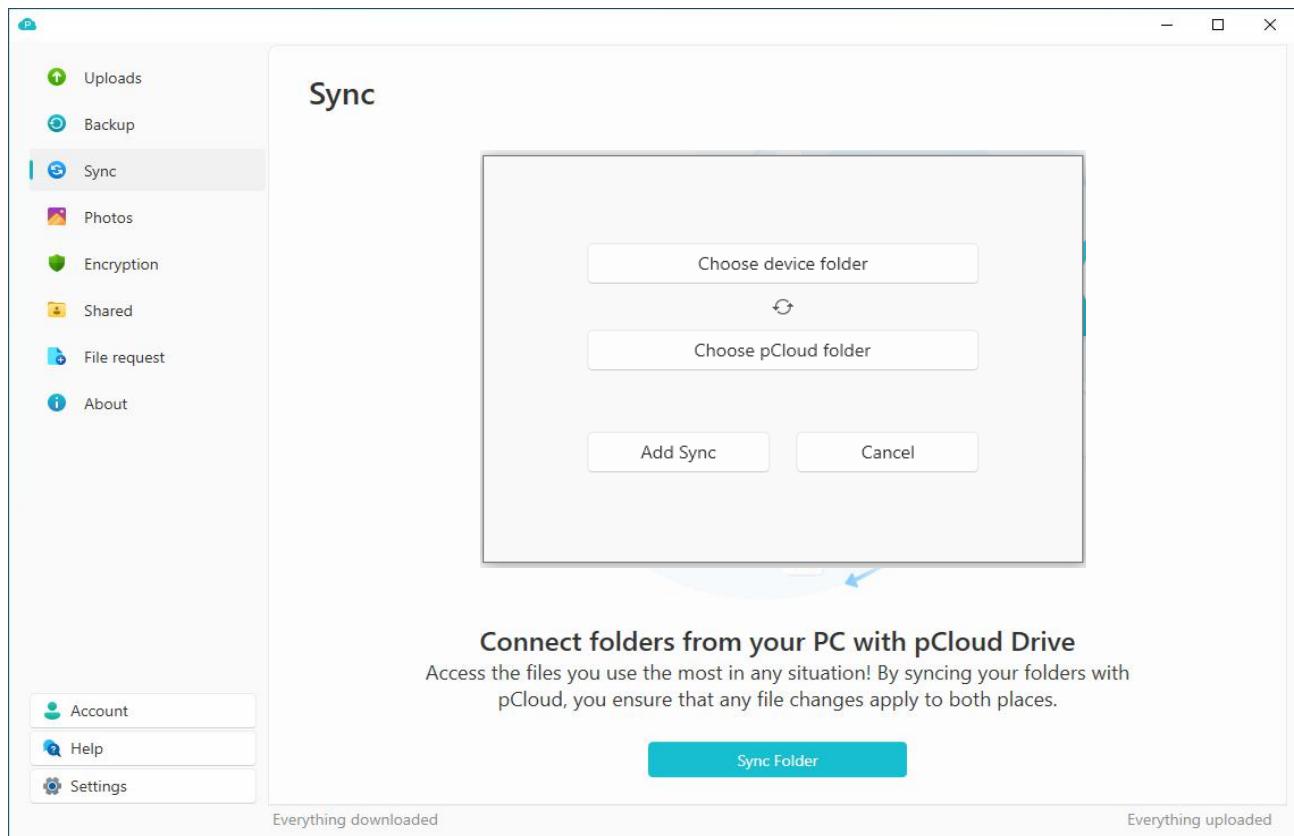


Figure 9 : PCloud Sync Setting

12.3 How to upload files through the website

- Click the Upload icon.
- Choose File upload or Folder upload.
- Click Browse for files or Pick folder.
- Select the files or folder and click Open.

You can also use Remote Upload, which lets you download files directly from a URL. Simply paste the link and click Upload. pCloud will download the file straight to your storage often at high speeds because it pulls the data directly from the source server.

12.4 How to upload files through PCloud Drive

Simply drag and drop, or copy any file or folder into the pCloud virtual drive or into a folder that is synced with pCloud.

12.5 How to retrieve your files

Recovering deleted files in pCloud is easy. Deleted items stay available for 15 days on the free plan, 30 days on premium plans, and up to 365 days with Extended File History. You can also permanently delete backups if needed.

12.6 Ease of use

pCloud is available for Mac, Windows, and Linux, and has a simple interface that's easy to use. You can upload files with the upload button or by dragging them in. It also provides easy file sharing and offers good upload/download speeds with a responsive interface.

12.7 Security and encryption

Utilizes encryption during data transfer to ensure that your files are and at the same time, data encryption across various locations of the server for better security. With, only you keep the keys, thus no access is permitted. Crypto is the subscription that adds an additional of protection for your and your password.

12.8 File versioning

With a selected expiration time, pCloud carefully stores the processes of the files' earlier versions and retrieves them according to the user's requirement. Using the Revisions feature, you can view and recover past versions of any file. Just click the gear icon, choose Revisions, and select the version you want.

File versions are stored for 15 days on the free plan and 30 days on Premium, Premium Plus, or Lifetime plans.

The pCloud Rewind feature lets you view your entire account as it existed at a specific date and time. If you accidentally delete shared content, Rewind allows you to restore or download all non-encrypted files.

12.9 How to use PCloud Transfer

pCloud Transfer lets you send files up to **5 GB** without needing a pCloud account. Just upload the files, enter up to 10 recipient emails, add your email and an optional message. The files are uploaded to pCloud's servers and can be downloaded by all recipients.

12.10 PCloud installation process

Download a PCloud exe and install by GUI by simply pressing the next and install the PCloud is open in the PC.

By default PCloud is Automatically cover almost all common folder like Desktop, Document, Download, Music, Picture, Video any new file is created it will automatically upload to PCloud and save it if we can delete the file it will go to recycle bin but the in PCloud it is stored.

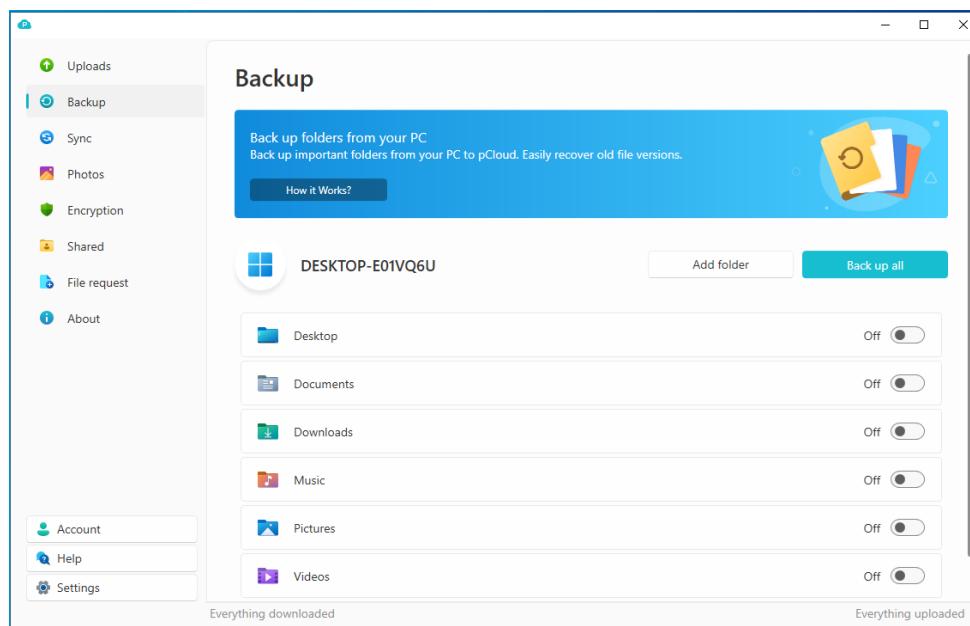


Figure 2 : PCloud Backup Folder

At free level the PCloud is give the **5 GB** storage plans is for the life time.

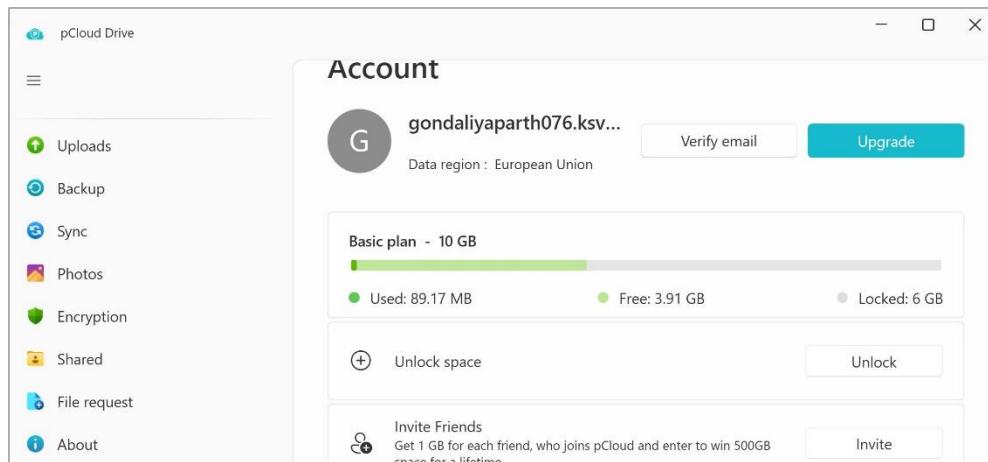


Figure 11 : PCloud 5 GB space Limited Setting

After installed the PCloud it will be create the new disk in the pc with the name PCloud and all storage are there in this drive with the crypt folder for the user private data store facility encrypted data.

It's file extinction exfat

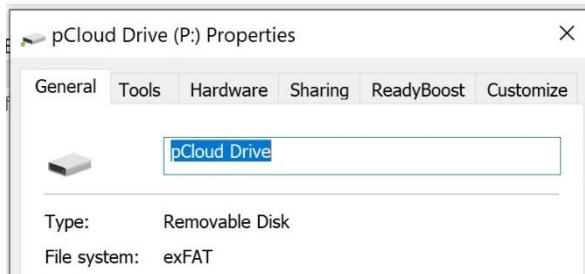


Figure 32 : PCloud Disk Extension

PCloud current version is the 5.0.8

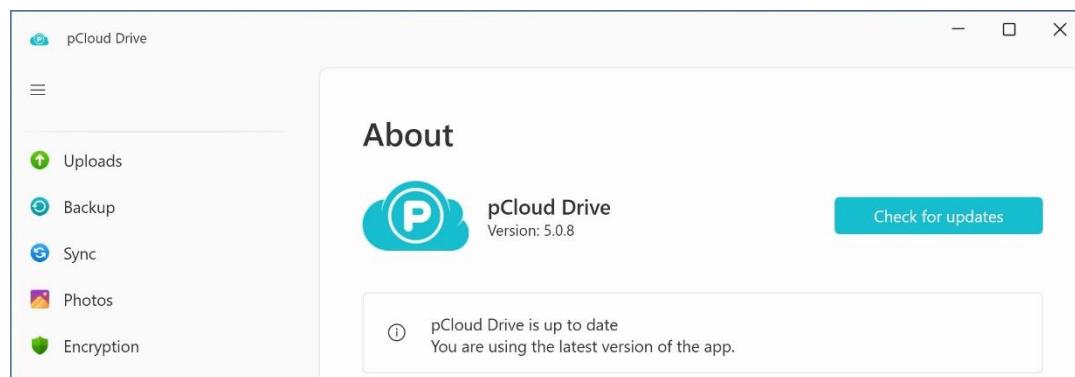


Figure 13 : PCloud Version

For the user private data storage in Encryption service is there for the premium user and free trial for the 15 day for all the user and the it's security is at top level, character upper-lower case, special symbol, numeric add password 8 char long that also it shown it is medium level strong that why also it will show the not a strong password.



Figure 44 : PCloud Encryption Folder

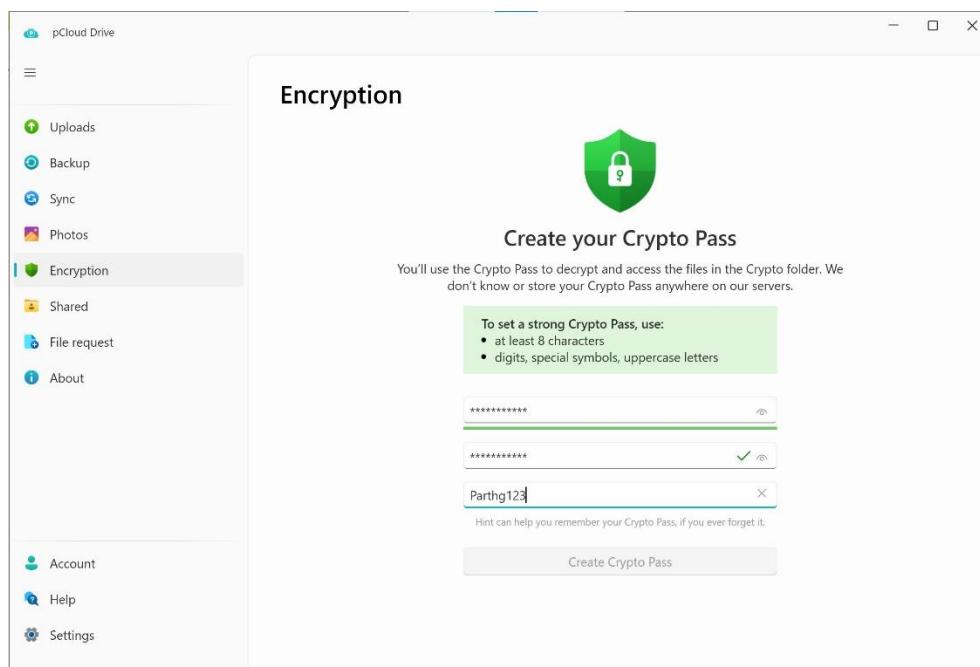


Figure 15 : PCLOUD Encryption Folder Setting

One drop back is there no password recovery is there.

For see the data of the crypto folder we can unlock from the application after we can see the data otherwise it will show that there is no data in this folder.

Figure 16 : PCLOUD Crypto folder empty in lock

Figure 5 : PCLOUD Encryption folder lock

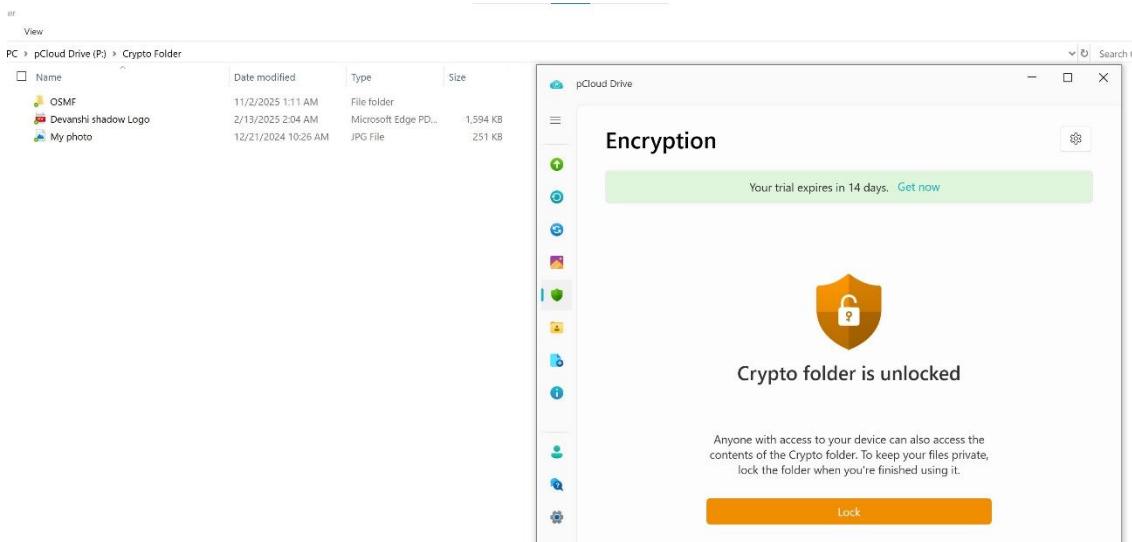


Figure 68 : PCloud crypto folder unlock



Figure 19 : PCloud size shown after unlock

Rewind helps you find and recover old versions of your files, removed shared work or files you accidentally moved to the Trash. Keep in mind, permanently deleted files cannot be recovered. Pick a date and time from the calendar above and rewind the time!

Want to extend Rewind? Get up to one year Extended File History as an add-on. But is work only in the browser by the paid offer only.

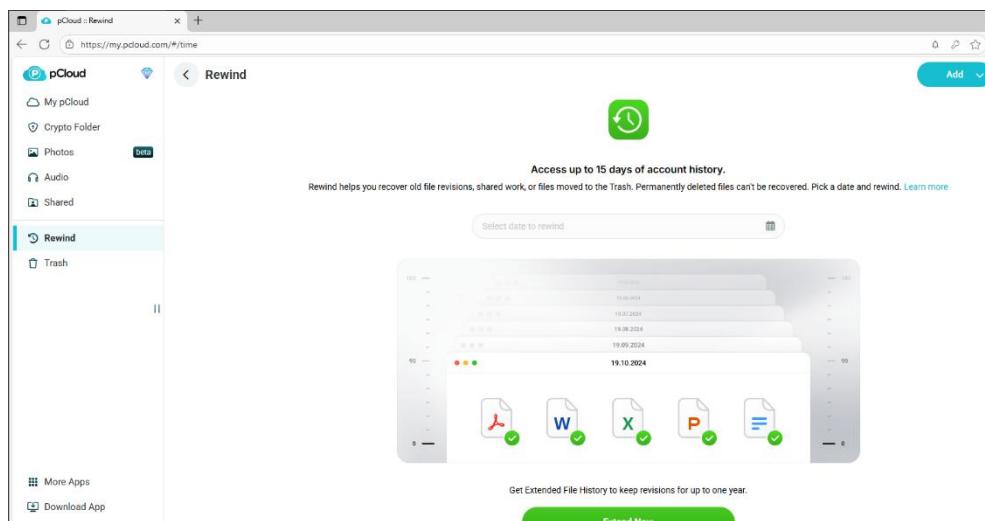


Figure 20 : Rewind state

12.11 RAM dump

RAM DUMP analysis by the FTK ram dump into Hex-Editor.

561277c0	28 00 00 00 00 00 80	80 c4 67 02	84 69 00 00	(.....€Äg..i..
561277d0	00 00 00 00 00 00 00	00 00 00 00 00 00	01 00 00 00	
561277e0	4e 65 77 20 6c 6f	67 69 6e 20 6f 6e	20 79 6f 75	New Login on you
561277f0	72 20 70 43 6c 6f	75 64 20 61 63 63	6f 75 6e 74	r pCloud account
56127800	20 2d 20 70 61 72	74 68 73 74 75 64	79 32 36 38	- parthstudy268
56127810	34 40 67 6d 61 69	6c 2e 63 6f 6d 20	2d 20 47 6d	4@gmail.com - Gm
56127820	61 69 6c 00 00 00	00 00 00 00 00 00	01 00 00 00	ail.....
56127830	00 00 00 00 03 52	4b f0 ff ff ff ff	fc ad b4 0fRKöyyyü..
56127840	6f 6d 2e 57 69 6e	72 74 41 70 70 49	64 53 65 72	om.WinrtAppIdSer

Figure 21 : Email Id shown in Ram Dump

Crypto folder password found by FTK Ram. DUMP

5ef9b2c0	00 06 0b f8 1a f0 9c a4	fa 1a 00 52 e8 84 4a 38	...øœøú..Rè,,J8
5ef9b2d0	1b 00 01 80 10 00 f4 20	07 b1 08 39 00 79 07 06	...€..ø .+ .9.v..
5ef9b2e0	41 00 0b 53 30 32 40 72	35 33 23 70 31 32 0b 2f	A. 502@r53#p12./
5ef9b2f0	08 b8 00 15 1e ff 1c f2	5d 24 90 8b 00 1d 60 48	.,...y.øJS..<..H
5ef9b300	14 a0 08 10 b0 c9 c5 fa	02 f0 c0 06 fa 1d 0e e8°EAú.øA.ú..è
5ef9b310	01 c0 d0 e0 f0 1d 6e 18	fc 71 03 10 6c 02 40 96	.Aðað.n.üq..l.-

Figure 22 : Crypto Password reveal in Ram Dump

Wireshark this cloud is also the fully encrypted so no one can get the anything from the wire share traffic hand shake is also encrypted.

22 9.616786	23.212.254.120	192.168.11.129	TLSv1.3	78 Application Data
37 22.222323	192.168.11.129	52.247.72.241	TLSv1.2	231 Client Hello (SNI=in.appcenter.ms)
39 22.525190	52.247.72.241	192.168.11.129	TLSv1.2	1514 Server Hello
42 22.525190	52.247.72.241	192.168.11.129	TLSv1.2	655 Certificate, Server Key Exchange, Server Hello Done
44 22.530149	192.168.11.129	52.247.72.241	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
46 22.827269	52.247.72.241	192.168.11.129	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
47 22.834229	192.168.11.129	52.247.72.241	TLSv1.2	960 Application Data
14585 397.535772	20.198.167.116	192.168.11.129	TLSv1.2	1514 Certificate
14586 397.535772	20.198.167.116	192.168.11.129	TLSv1.2	1112 Certificate Status, Server Key Exchange, Server Hello Done
14588 397.547497	192.168.11.129	20.198.167.116	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
14590 397.613896	20.198.167.116	192.168.11.129	TLSv1.2	413 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
14592 397.615887	192.168.11.129	20.198.167.116	TLSv1.2	141 Application Data
14594 397.616357	192.168.11.129	20.198.167.116	TLSv1.2	92 Application Data
14596 397.617395	192.168.11.129	20.198.167.116	TLSv1.2	320 Application Data

Figure 23 : Encrypted hand shake

12.12 Disk analyses

Name	S	C	O	Modified Time	Change Time
[current folder]				2025-11-06 15:35:36 IST	2025-11-06 15:35:36 IST
[parent folder]				2025-11-07 12:27:51 IST	2025-11-07 12:27:51 IST
Cache				2025-11-06 16:08:10 IST	2025-11-06 16:08:10 IST
EBWebView				2025-11-06 15:36:03 IST	2025-11-06 15:36:03 IST
ntfthumbs				2025-11-06 15:33:59 IST	2025-11-06 15:33:59 IST
data.db	▼	0		2025-11-07 12:18:39 IST	2025-11-07 12:18:39 IST
data.db-shm		0		2025-11-07 12:18:36 IST	2025-11-07 12:18:36 IST
data.db-wal	▼	0		2025-11-07 12:18:39 IST	2025-11-07 12:18:39 IST
wpflog.log	▼	0		2025-11-07 12:18:43 IST	2025-11-07 12:18:43 IST

Figure 24 :7 Pcloud DB Folder

We can find the data base of the PCloud in where the all the user interaction are be save in this file with user email id we can see all the file upload data entry and deleted entry are there with their prices location, created and modified time entry.

Table setting		50 entries	Page 1 of 1	Exp
id	value			
vivapcloud	0			
username	parthstudy2684@gmail.com			
userid	5816199			
usedquota	105709438			
upscreenslinks	0			
upscreensexpires	0			
startminimized	0			
saveauth	1			
runstatus	1			
registered	1762421744			
randomhashf	fcbdfeb9630fe79a0c944b54ce9f3630b49fb5bd8347cff			

Figure 25 : Pcloud DB find used id

Table setting		50 entries
id	value	
setting		
folder		
file		
filerevision	11/6/2025 5	
syncfolderdelayed	1	
syncfolder	1	
localfolder		
Theme	sqlite_sequence	
api_server	bineapi.pclo	
auth	zOIVPVZnVt	
business		

Figure 26 : Pcloud DB Table

Table folder		7 entries	Page 1 of 1	Export to CSV				
id	parentfol...	userid	permиси...	name	ctime	mtime	flags	subdircnt
0						1762424651	0	6
20067888147	0	5816199	15	My Music	1762421744	1762421744	0	0
20067888149	0	5816199	15	My Pictures	1762421744	1762421744	0	0
20067888150	0	5816199	15	My Videos	1762421744	1762421744	0	0
20068471815	0	5816199	15	System Volume Information	1762423536	1762423536	0	0
20068596141	0	5816199	15	Crypto Folder	1762423878	1762423878	1	0
20068841339	0	5816199	15	pCloud Backup	1762424651	1762424689	0	0

Figure 27 : List of all Folder sync with PCloud

Continually we book the evidence in autopsy so that our report are look good with price evidence details.

Table		file	16 entries		Page 1 of 1		Export to CSV					
id	parentfolde...	userid	size	hash	flags	△ name	ctime	mtime	category	thumb	icon	art
77974983326	20068841339	5816199	10962360	768167196..0		ChromeSetup.exe	176240966..	176240967..0		0	executable	
77970030652	20067888147	5816199	1442376	-38583791..0		Demo Audio 2.mp3	176242174..	176242174..3		0	audio	
77974543172	20068596141	5816199	264184	-91773901..0		GU5YKKRVANYLAM2WJYW6NA...	176241525..	176241525..0		0	file	
77970030601	0	5816199	16371465	548473439..0		Getting started with pCloud.pdf	176242174..	176242174..4		0	document	
77970030656	20067888147	5816199	6698872	565527674..0		GotJoy.mp3	176242174..	176242174..3		0	audio	
77970030663	20067888147	5816199	28096964	-83191098..0		Lovely Day.wav	176242174..	176242174..3		0	audio	
77970030668	20067888147	5816199	11252576	464549959..0		Momentum.mp3	176242174..	176242174..3		0	audio	
77974542403	20068596141	5816199	22511072	276527906..0		SXLXJATHR34L7APSYBLCXJZIFF5..	176241992..	176241992..0		0	file	
77972319751	20068471815	5816199	12	-33849626..0		WPSSettings.dat	176242353..	176242353..0		0	file	
77970030615	20067888149	5816199	666846	-90407254..0		friends.jpg	176242174..	176242174..1		1	image	
77970030625	20067888149	5816199	189628	-86337839..0		happy-family.jpg	176242174..	176242174..1		1	image	
77970030633	20067888149	5816199	32905	397856546..0		in-the-sky.jpg	176242174..	176242174..1		1	image	

Figure28 : Pcloud Files Sync List

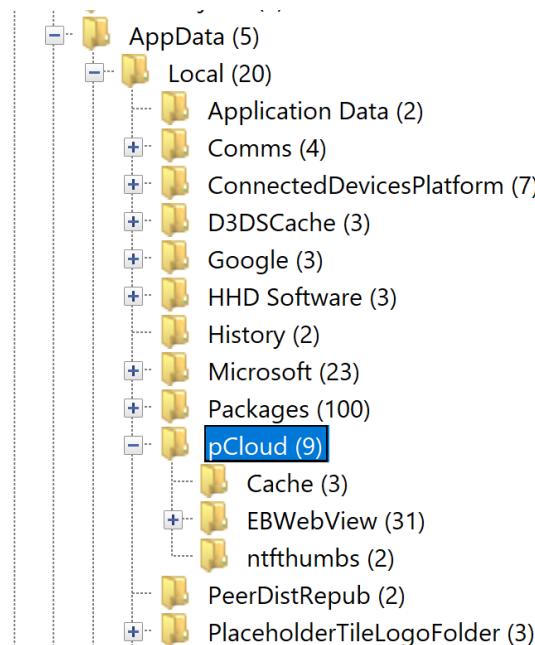


Figure 29 : Pcloud Hidden Folder

12.13 Browser data artifact

- ⚡ Web Cache (3558)
- 🍪 Web Cookies (256)
- 📁 Web Downloads (118)
- 📄 Web Form Autofill (359)
- ⏳ Web History (1967)
- 🔎 Web Search (61)

Figure 30 : Total Browser History Found

Source Name	S	C	O	URL	△ Date Accessed	Title
History			5	https://accounts.google.com/ServiceLo...	2025-11-06 15:36:22 IST	Inbox (160) - parthstudy2684@gmail.com - Gmail
History			5	https://mail.google.com/accounts/SetO...	2025-11-06 15:36:22 IST	Inbox (160) - parthstudy2684@gmail.com - Gmail
History			5	https://mail.google.com/mail/u/0/?tab...	2025-11-06 15:36:22 IST	Inbox (160) - parthstudy2684@gmail.com - Gmail
History			5	https://mail.google.com/mail/u/0/?ogbl...	2025-11-06 15:36:22 IST	Inbox (160) - parthstudy2684@gmail.com - Gmail
History			5	https://mail.google.com/mail/u/0/?ogbl... 2025-11-06 15:36:30 IST	2025-11-06 15:36:30 IST	New login on your pCloud account - parthstudy2684@gmail.com - Gmail
History			5	https://mail.google.com/mail/u/0/?ogbl... 2025-11-06 15:36:30 IST	2025-11-06 15:36:30 IST	New login on your pCloud account - parthstudy2684@gmail.com - Gmail
History			5	https://www.google.com/url?q=https://...	2025-11-06 15:36:35 IST	

Figure 31 : Browser History email verify for Pcloud Service

We find the history of the user there the mail id is verified with the PCloud service means that the user use the PCloud service for the store the data.

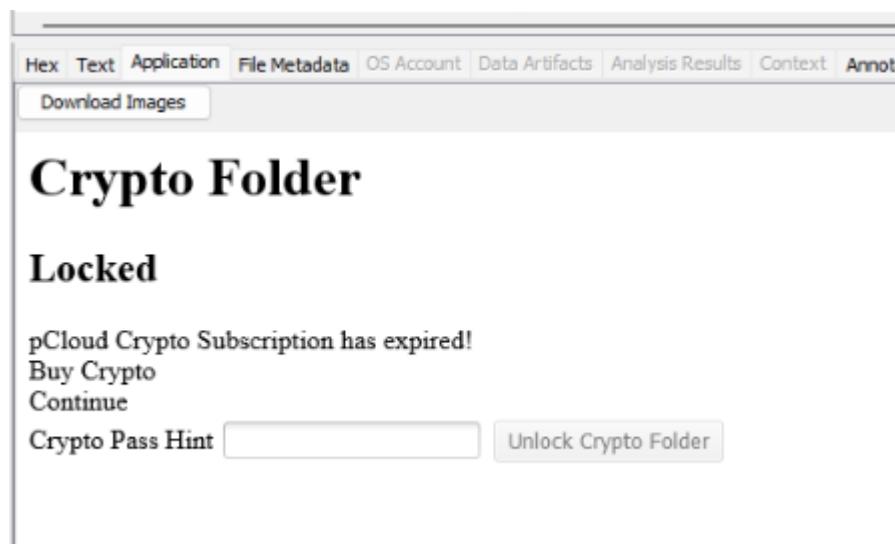


Figure 32 : Cache Preview of crypto folder

From the browser cache data we can find the loaded screen with crypto folder means that user store the private data in the crypto folder for hide the data from the normal users.

Result: 4 of 47 Result	
Type	Value
Program Name	pCloud Drive v.5.0.10.0
Date/Time	2025-11-06 09:39:21 IST
Source File Path	/img_Windows 10 Pcloud.vmdk/vol_vol6/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775706

Figure 33 : Pcloud Version

We can find the version of the PCloud is used by user for the data store.

We can also find PCloud login data store by browsers accounts with Username.

Type	Value	Source(s)
URL	https://www.pcloud.com/	Recent Activity
Date Created	2025-11-06 15:05:50 IST	Recent Activity
Decoded URL	pcloud.com	Recent Activity
Username	parthstudy2684@gmail.com	Recent Activity
Realm	https://www.pcloud.com/	Recent Activity
Domain	pcloud.com	Recent Activity
Program Name	Google Chrome	Recent Activity
Username	Default	Recent Activity
Source File Path	/img_Windows 10 Pcloud.vmdk/vol_vol6/Users/pCloud/AppData/Local/Google/Chrome/User Data/Default/Login Data	
Artifact ID	-9223372036854773633	

Figure 34 : Pcloud Login data

After doing find all evidence we can create a report in HTML file.

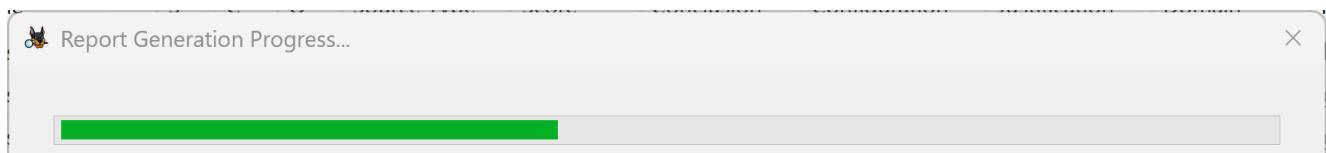


Figure 35 : Report created by the Autopsy

Installed Extensions			
Extension Name	Description	Version	App ID
StorageAce	Easily manage Cookies, Local Storage and Session Storage for the selected sites	2.9.10	cpbgcbmddckpmhfbdckeolkhh
Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	nmmhkkegcagldgimedpiccm
pCloud Save	Save your favorite web images, videos, text and more to pCloud - up to 100GB	2.0.1	npamdkabjnccnoaoafdjcaipmncc

Figure 36 : Extention installed

site setting (hsts)	2025-11-06 01:33:58.525	Encoded domain: EUee8fEWEJXzg9tS5msIIFKED/eSKlh6OyfShJAx5qg= HSTS observed	{'expiry': 1793957638.525803, 'host': 'EUee8fEWEJXzg9tS5msIIFKED/eSKlh6OyfShJAx5qg= HSTS observed'}
url	2025-11-06 01:34:00.355	https://www.pcloud.com/	pCloud - File Security Made Simple pCloud
site setting (hsts)	2025-11-06 01:34:04.878	Encoded domain: RNSljhzOrppvtsaSJ2jzGCoQt5mAXe0MwsljeUlk20= HSTS observed	{'expiry': 1793957644.878906, 'host': 'RNSljhzOrppvtsaSJ2jzGCoQt5mAXe0MwsljeUlk20= HSTS observed'}
site setting (hsts)	2025-11-06 01:34:27.395	Encoded domain: 50fvKe0UnlwQ0FaadZ0bixu8eZ5Fhj29nHjeOXIA: HSTS observed	{'expiry': 1793957667.395804, 'host': '50fvKe0UnlwQ0FaadZ0bixu8eZ5Fhj29nHjeOXIA: HSTS observed'}
site setting (hsts)	2025-11-06 01:34:28.763	Encoded domain: nPMi9yOfzAs8CJA0P+HpxvYNO4gwQluctXsoxO6H HSTS observed	{'expiry': 1793957668.763857, 'host': 'nPMi9yOfzAs8CJA0P+HpxvYNO4gwQluctXsoxO6H HSTS observed'}
autofill	2025-11-06 01:35:28.000		email parthstudy2684@gmail.com
site setting (modif)	2025-11-06 01:35:30.122	http://pcloud.com:80,*	password_protection [In Pre: {'last_modified': '13406895330122756', 'setting': {'password_on_focus_change': true}}]
login (username)	2025-11-06 01:35:34.102	https://www.pcloud.com/	parthstudy2684@gmail.com
login (saved cred)	2025-11-06 01:35:50.460	https://www.pcloud.com/	parthstudy2684@gmail.com
url	2025-11-06 01:35:56.386	https://www.pcloud.com/how-to-install-pcloud-drive-windows.htm	pCloud - File Security Made Simple pCloud
download	2025-11-06 01:36:09.780	https://def3.pcloud.com/cBZ7jtiz77Zicpgc97ZZZ4EdY0kZAKZZ35FzkZY	Complete - 100% [113782768 C:\Users\pCloud\Downloads\pCloud_Windows_5.0.10_x64.exe]
url	2025-11-06 01:36:15.061	https://my.pcloud.com/	pCloud :: File Manager

Figure 37 : Login history with email id and time-stamp

13. Mega sync

MEGASync is an intuitive software developed by MEGA Limited that allows you to easily synchronize folders across multiple computers. Once you upload your files to the cloud, you can access the same content on your drive within seconds. You can choose to sync your entire MEGA account or set up multiple selective syncs between specific folders on your computer and your MEGA storage. Deleted files are moved to special recovery folders both locally and in your MEGA account, making it easy to restore them if needed. MEGASync also works smoothly with your browser, helping manage MEGA file transfers more efficiently.

MEGA was built on the principle that encryption should not reduce usability. The service is fully accessible without requiring any software installation and remains the only cloud storage provider offering high-performance, end-to-end encryption directly in the browser. The only visible signs of MEGA's encryption system are the entropy collection during signup, the lack of a password reset option, and the unique browser-dependent methods used for file transfers.

Today, millions of users—both personal and business—trust MEGA to securely store and deliver massive amounts of data. MEGA's success comes from making strong security simple and easy to use. MEGASync is available through the web interface, desktop app, mobile apps, and even a command-line tool, making it accessible anywhere, anytime. The service supports Windows, macOS, and Linux, and offers 50 GB of free storage upon signup.

13.1 Installation process

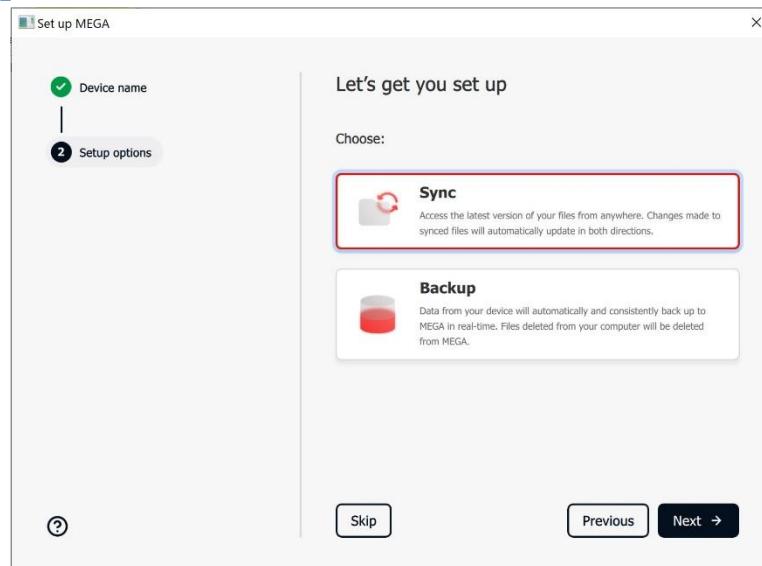


Figure 38 : Mega setup Installation

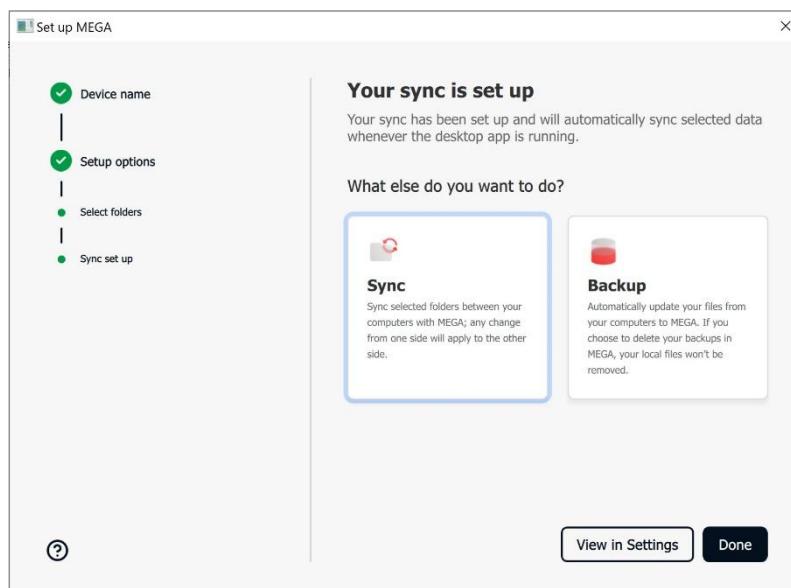


Figure 39 : Sync Setting

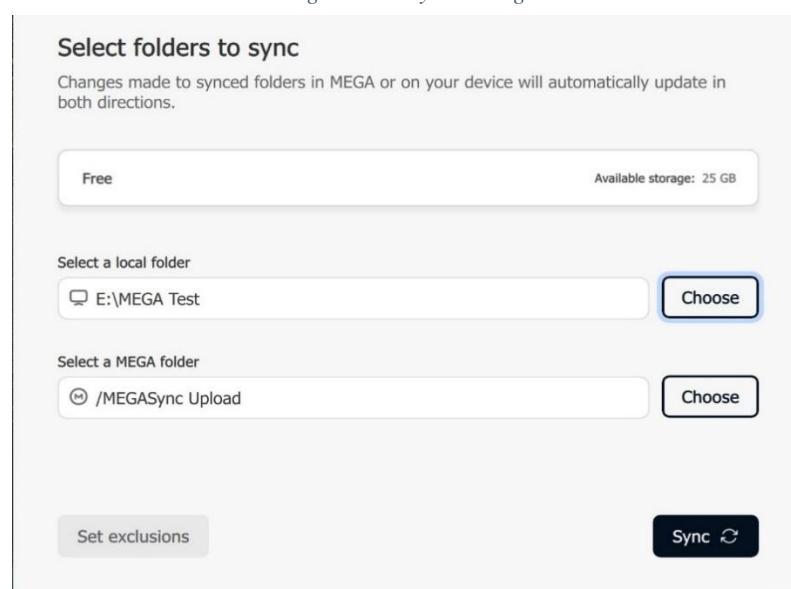


Figure 40 : Sync folder selection

It's simple just login in the mega cloud and download a.exe file and simply next.. Next and install.

In the starting it will be ask for the location where we create a folder of the mega cloud to store his data and sync folder.

It will ask for the full sync or selective sync means we can sync only important folder of all folder.

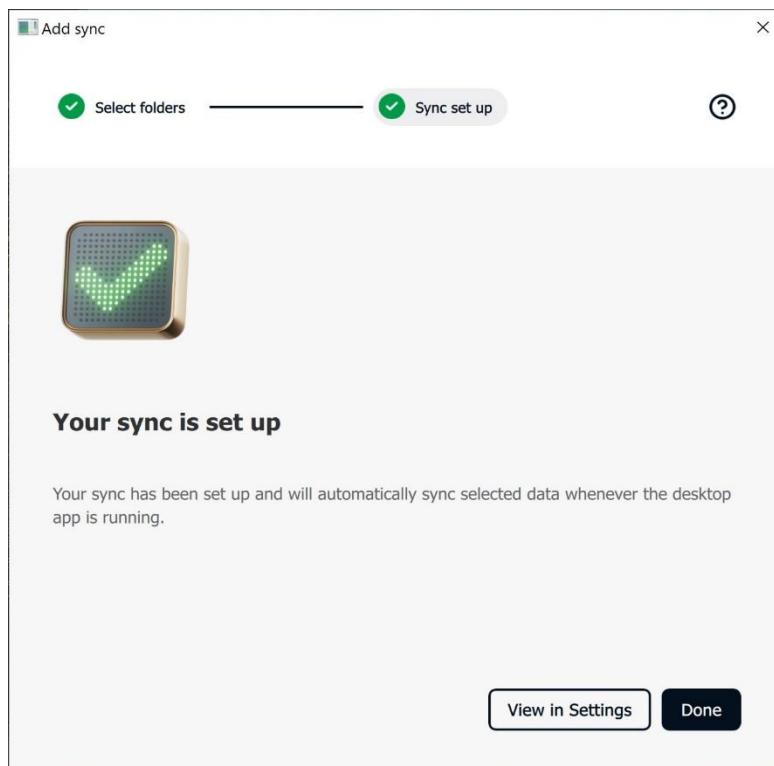


Figure 41 : Complete Setup

After a few second the installation is success install the mega cloud in the PC.

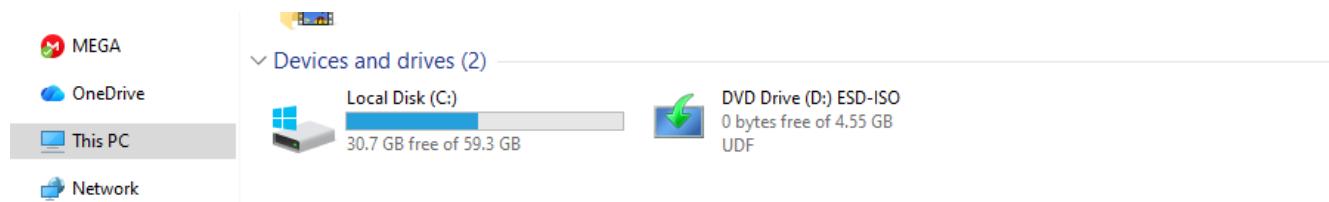


Figure 42 : No Local Disk

In this no disk is created in the this pc just it will give the folder to store the files in the pc and all are worked in the slide notification app that MegaSync in open for the user interaction.

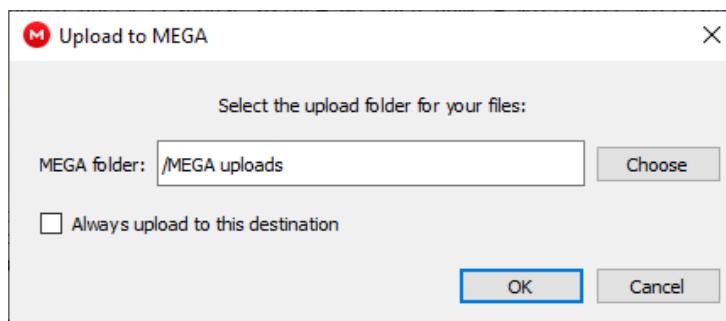


Figure 43 : Sync Folder Setting

We can use the multiple folder for the sync for the upload the data into a cloud

13.2 RAM dump

RAM dump analysis in the 1 cloud user client app is see that is not spared the user password to the ram dump also even if the new password change and immediately create that why also there is no trace in the ram dump of the password only the user id is shown all are in the encrypted.

It is most secured but for forensic analysis it is most difficult to find the user password.

2ac38af0	00	00	00	00	00	00	f4	78	c8	cc	00	43	00	80ôxEI.C.€	
2ac38b00	43	3a	5c	55	73	65	72	73	5c	4d	45	47	41	5c	C:\Users\MEGA\AppData\Local\Mega Limited\MEGAsync\avatars\gondaliyaparth076.csv@gmail.com.jpg...	
2ac38b10	70	44	61	74	61	5c	4c	6f	63	61	6c	5c	4d	65ixñI.D.€	
2ac38b20	20	4c	69	6d	69	74	65	64	5c	4d	45	47	41	73	79	6e
2ac38b30	63	5c	61	76	61	74	61	72	73	5c	67	6f	6e	64	61	6c
2ac38b40	69	79	61	70	61	72	74	68	30	37	36	2e	6b	73	76	40
2ac38b50	67	6d	61	69	6c	2e	63	6f	6d	2e	6a	70	67	00	00	00
2ac38b60	00	00	00	00	00	00	00	00	ed	78	f1	cc	00	44	00	80

Figure 44 : Email id Found

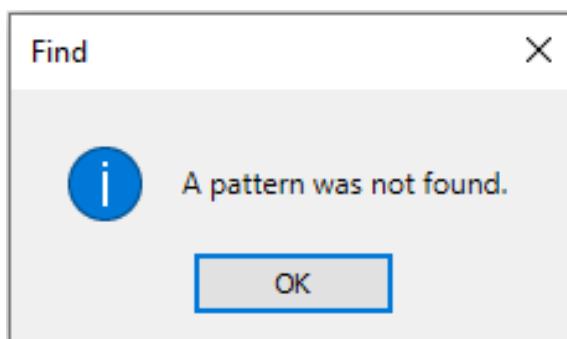


Figure 45 : Password not found

Password is not cached by the FTK Ram dump and the dd, task manager ram dump also the password is not there in the RAM.

```

11/07-06:20:44.903725 4368 DBG Qt Debug: false
11/07-06:20:44.903730 4368 DBG Qt Context: default 2
11/07-06:20:44.926838 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGAsync/Resources_common.rcc
11/07-06:20:44.926903 4368 DBG Qt Debug: false
11/07-06:20:44.926912 4368 DBG Qt Context: default 2
11/07-06:20:44.936136 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGAsync/Resources_qml.rcc
11/07-06:20:44.936187 4368 DBG Qt Debug: false
11/07-06:20:44.936192 4368 DBG Qt Context: default 2
11/07-06:20:44.940785 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGAsync/qml.rcc
11/07-06:20:44.940829 4368 DBG Qt Debug: false
11/07-06:20:44.940832 4368 DBG Qt Context: default 2
11/07-06:20:44.948083 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGAsync/Resources_light.rcc
11/07-06:20:45.281392 4368 DBG libuv version: 1.49.2 [megaapi_impl.cpp:6931]
11/07-06:20:45.286566 8472 ERR Could not open pipe. Error Code=2 The system cannot find the file specified. [comms_client.cpp:50]
11/07-06:20:45.286726 8472 ERR runShutdown Couldn't connect [client.cpp:53]
11/07-06:20:45.286735 8472 DBG Process::Process(""):"C:/Users/MEGA/AppData/Local/MEGAsync/mega-desktop-app-gfxworker.exe" -n=cecf52bc-7979-4e37-ad80-24a9d9aa
11/07-06:20:45.287103 8472 DBG cmdLine = ''C:/Users/MEGA/AppData/Local/MEGAsync/mega-desktop-app-gfxworker.exe" -n=cecf52bc-7979-4e37-ad80-24a9d9aa4f78 -l=
11/07-06:20:45.291703 4368 DBG curl version: 8.14.1-DEV [net.cpp:209]
11/07-06:20:45.291706 4368 DBG SSL version: Schannel [net.cpp:214]
11/07-06:20:45.292374 4368 DBG libz version: 1.3.1 [net.cpp:238]

```

Figure 46 : Log Files

All log are saved into the txt file to easy analysis and in log files also the password is not there only user id is there with proper date and time.

C:\Users\MEGA\AppData\Local\Mega Limited\MEGAsync\logs

C:\Users\MEGA\AppData\Local\Mega Limited\MegaSync

Megaclient_statecache13_MUtpdmdEVFNwa29Hm1_kX2DXDE95GAmM7Efs and its DB name is also encrypted and we can see the some crypto error f in the dB also we can find the list of the data entry are done in the Mega cloud.

Table: nodes													
nodehandle	parenthandle	name	fingerprint	origFingerprint	type	size	share	fav	mimetype	ctime	flags	counter	node
1	3868965914693	-1	CRYPTO_ERROR	BLOB		3 4294967295	0	0	0 1687692556 0	BLOB	BLOB		
2	143650689403637	18259925636	Welcome to MEGA.pdf	BLOB		0 969609	0	0	4 1687692561 0	BLOB	BLOB		
3	222800691780113	70423527430672	Self Photo.jpg	BLOB		0 26018	0	0	1 1687693549 0	BLOB	BLOB		
4	100752619359268	168234138634384	LAB - 6_Malware Analysis From File & ...	BLOB		0 392275	0	0	4 1687693553 0	BLOB	BLOB		
5	88136169740996	168234138634384	malware 1.pdf	BLOB		0 3131235	0	0	4 1687693554 0	BLOB	BLOB		
6	168234138634384	20377692686900	doc	BLOB		1 4294967295	0	0	0 1687693547 0	BLOB	BLOB		
7	9940033116853	168234138634384	Prajapati Himil Harshadkumar.pdf	BLOB		0 171914	0	0	4 1687693555 0	BLOB	BLOB		
8	70423527430672	20377692686900	photos	BLOB		1 4294967295	0	0	0 1687693547 0	BLOB	BLOB		
9	140918014529137	70423527430672	provisnal certificate.jpg	BLOB		0 2204770	0	0	1 1687693555 0	BLOB	BLOB		
10	143719474976949	215043782216276	cat-g62b035a58_1920.jpg	BLOB		0 379351	0	0	1 1687696537 0	BLOB	BLOB		
11	22223415967397	215043782216276	hd-wallpaper-g69e16c2d8_1920.jpg	BLOB		0 362830	0	0	1 1687696537 0	BLOB	BLOB		
12	618697738917	215043782216276	hd-wallpaper-g5930fa13_1920.jpg	BLOB		0 526890	0	0	1 1687696537 0	BLOB	BLOB		
13	150293070650085	215043782216276	hd-wallpaper-g58f7e4a77_1920.jpg	BLOB		0 550209	0	0	1 1687696538 0	BLOB	BLOB		
14	215043782216276	20377692686900	SAMPLE STUFF	BLOB		1 4294967295	0	0	0 1687696532 0	BLOB	BLOB		
15	91907136196304	215043782216276	waterfall-37088.mp4	BLOB		0 32026769	0	0	3 1687696541 0	BLOB	BLOB		
16	10008756526181	215043782216276	blooms-113004.mp4	BLOB		0 7016467	0	0	3 1687696536 0	BLOB	BLOB		
17	91474617227265	215043782216276	seoul-21985.mp4	BLOB		0 3238956	0	0	3 1687696538 0	BLOB	BLOB		
18	141994189921937	18259925636	Demo Audio 2.mp3	BLOB		0 1442376	0	0	2 1687693554 0	BLOB	BLOB		
19	73833999523329	18259925636	GotJoy.mp3	BLOB		0 6698872	0	0	2 1687693551 0	BLOB	BLOB		
20	71634756360705	18259925636	Lovely Day.wav	BLOB		0 28096964	0	0	2 1687693558 0	BLOB	BLOB		
21	18259925636	-1	CRYPTO_ERROR	BLOB		2 -2	0	0	0 1687692556 0	BLOB	BLOB		
22	20377692686900	18259925636	MEGAsync Uploads	BLOB		1 -1	0	0	0 1687693546 0	BLOB	BLOB		
23	80841441037877	18259925636	Momentum.mp3	BLOB		0 11252576	0	0	2 1687693557 0	BLOB	BLOB		
24	168905297382500	89699342371456	Demo Audio 2.mp3	BLOB		0 1442376	0	0	2 1687697729 2	BLOB	BLOB		
25	10608989751872	-1	CRYPTO_ERROR	BLOB		4 -4	0	0	0 1687692556 0	BLOB	BLOB		
26	89699342371456	215221013978804	2023-06-25	BLOB		1 4294967295	0	0	0 1687697764 2	BLOB	BLOB		

Figure 47 : Sync DB

MEGA													
access	top	loads	ments	res	Name	#	Title	Contributing artists	Album				
					.megaignore								
					Chal Chaiya Chaiya								
					Chikni Chameli								
					HVME - Goosebumps (8D AUDIO)								
					Na Kajre Ki Dhar								

Figure 48 : List of files are Synced in Cloud

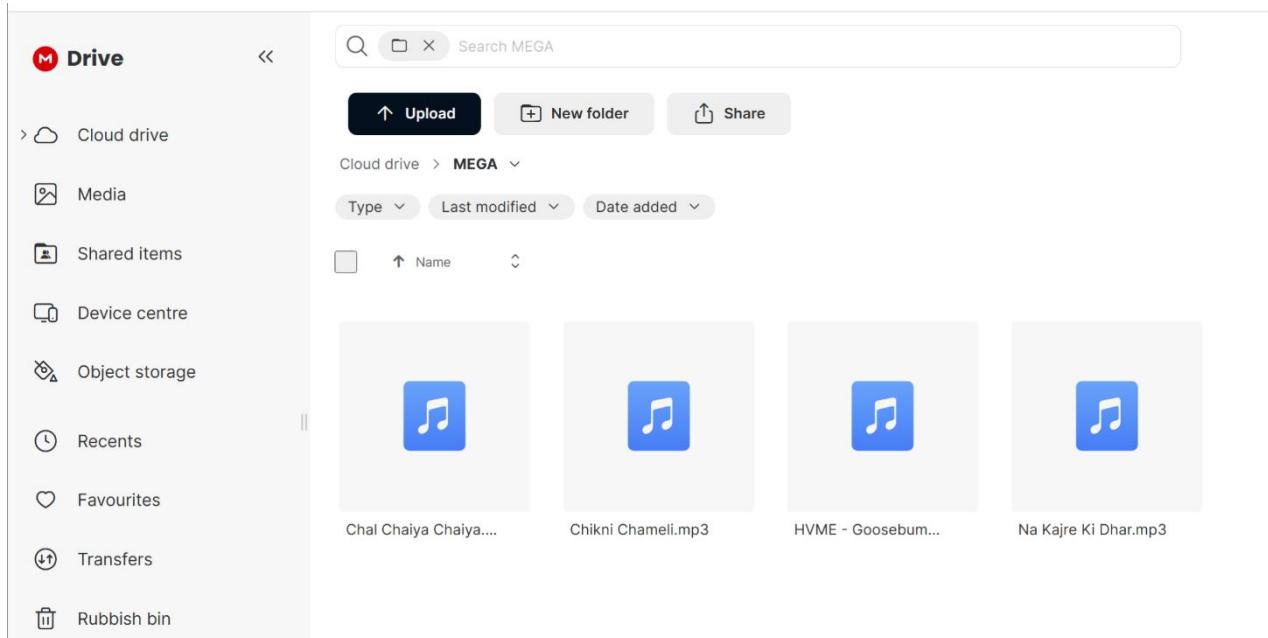


Figure 49 : Browser view of cloud

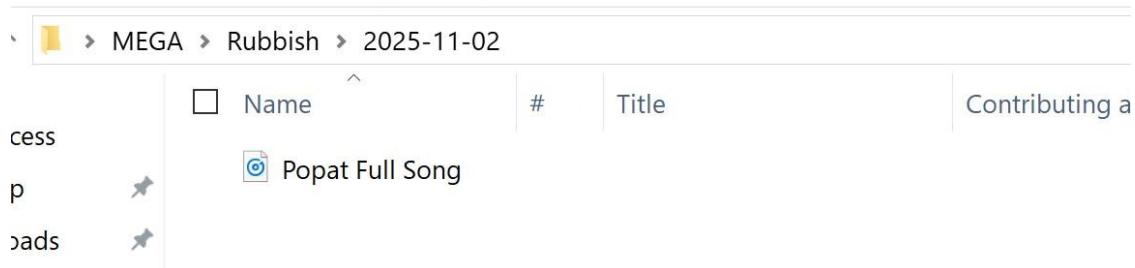


Figure 50 : Files deleted from cloud effect the PC

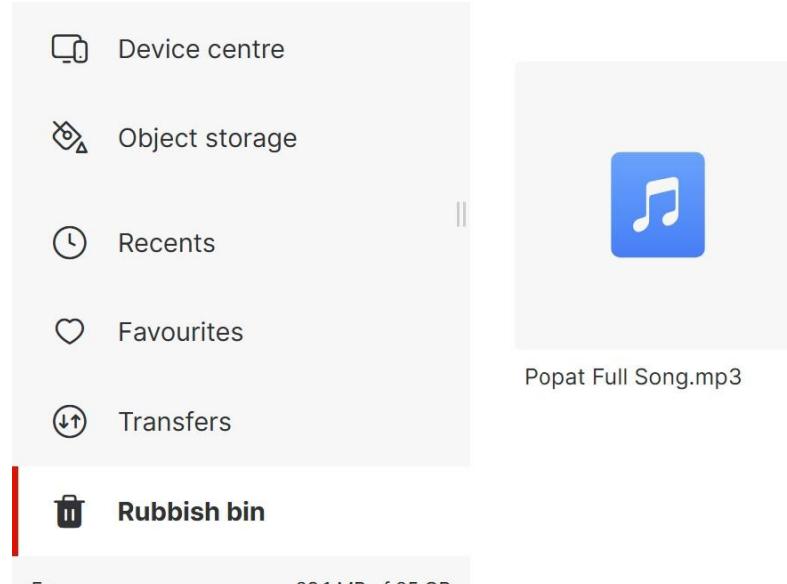


Figure 51 : Same effect on browser

ALL stuff are real time sync and if we can delete the file from the pc and three in the cloud we can see the real time select and that file also be the delete in the cloud and that file in also in the trash in cloud as will in the pc also.

An if we can restore from the cloud so we can get the file back in the folder and the another file is also there in the recycle bin.

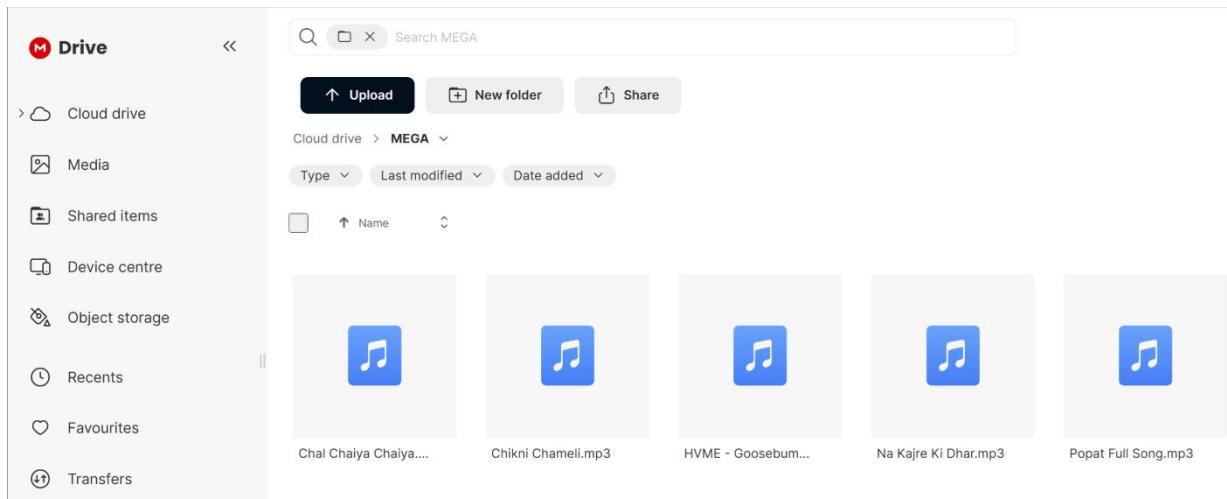


Figure 52 : Restore files from the cloud recycle

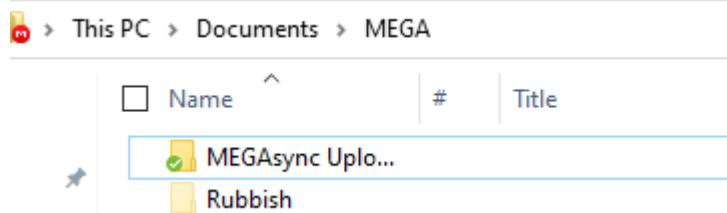


Figure 53 : New file is created in the Folder

File sync we can capture in ram dump with the file name.

011f1fc0	6d 65	6e 74	20 3d	3d 3d	e sequential Element =====						
011f1fd0	3d 3d	=====									
011f1fe0	3d 2d	2d 3e	0d 0a	3c 21	45 4e	54 49	54 59	20 25			-->..<!ENTITY %
011f1ff0	20 73	65 71	2d 63	6f 6e	74 65	6e 74	20 22	25 63			seq-content "%c
011f2000	4d 45	47 41	7b 22	63 22	3a 22	41 37	6e 64	55 55			MEGA{"c":"A7ndUU
011f2010	6f 55	77 33	67 30	4d 57	5f 35	45 4c	2d 74	73 67			oUw3gOMW_5EL-tsg
011f2020	53 57	4c 70	68 6b	22 2c	22 6e	22 3a	22 4d	45 47			SWLphk","n": "MEG
011f2030	41 73	79 6e	63 2e	44 4d	50 22	7d 00	00 00	00 00			Async.DMP"}.....
011f2040	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00		

Figure 54 : Encrypted file sync

Wire share this cloud is also the fully encrypted so no one can get the anything from the wire share traffic hand shake is also encrypted

25725	152.495298	66.203.124.146	192.168.11.130	TLSv1.2	79 Application Data
25732	153.432370	192.168.11.130	51.11.168.232	TLSv1.2	270 Client Hello (SNI=settings-win.data.microsoft.com)
25734	153.569924	51.11.168.232	192.168.11.130	TCP	1514 443 + 50489 [ACK] Seq=1 Ack=217 Win=64240 Len=1460 [TCP PDU reassembled in 25736]
25736	153.569924	51.11.168.232	192.168.11.130	TLSv1.2	892 Server Hello, Certificate, Server Key Exchange, Server Hello Done
25738	153.576909	192.168.11.130	51.11.168.232	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
25740	153.712250	51.11.168.232	192.168.11.130	TLSv1.2	174 Change Cipher Spec, Encrypted Handshake Message, Application Data
25741	153.717376	192.168.11.130	51.11.168.232	TLSv1.2	141 Application Data

Figure 55 : Encrypted hand shake

13.3 Disk analysis

Open the .vmdk file of the mega drive in the autopsy and it take a time for load the disk and finally loaded in the autopsy.

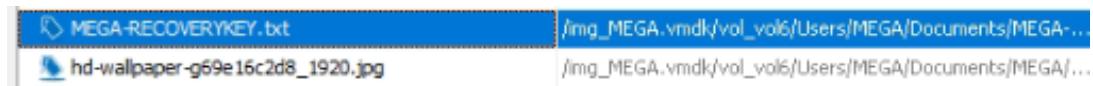


Figure 56 : Cloud Recovery key

We can find the recover key to recover the cloud.

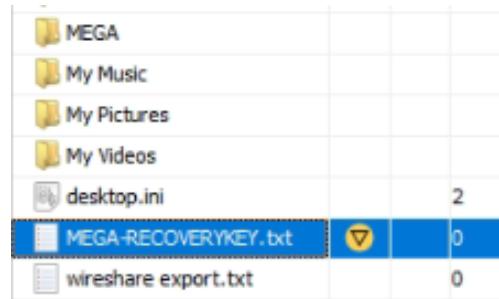


Figure 57 : 8Book Mark the key

Name	S	C	O	Modified Time	C
[current folder]				2025-11-07 11:51:38 IST	2
[parent folder]				2025-11-07 11:50:45 IST	2
Rubbish				2025-11-07 11:51:30 IST	2
.megaignore	1			2025-11-07 11:51:30 IST	2
Chal Chaiya Chaiya.mp3	0			2025-09-29 21:55:12 IST	2
Chikni Chameli.mp3	0			2025-09-29 21:56:06 IST	2
desktop.ini	1			2025-11-07 11:51:30 IST	2
HVME - Goosebumps (8D AUDIO).mp3	0			2025-09-29 21:52:00 IST	2
Na Kajre Ki Dhar.mp3	0			2025-09-29 21:54:10 IST	2

Figure 58 : Deleted file and sync file list

We can find the deleted files also from the cloud via browser also we can find the data deleted from the disk.

	3	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	1632493	Allocated	Allocated	unkn
Evolution of Chrome Databases (v35).pdf	3	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	350402	Allocated	Allocated	unkn
Hindsight User Guide v1.3.0.pdf	3	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	2025-11-07 12:11:33 IST	350402	Allocated	Allocated	unkn

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Hindsight User Guide
Internet History Forensics for Google Chrome

Hindsight Version: 1.3.0
Author: Ryan Benson
Date: 2014-11-10

Figure 59 : Confirmed use of the Mega cloud

We can see the welcome pdf guide in the disk means that user is pretty sure that it use the mega cloud in this device.

History			2025-11-06 10:05:21 IST	2025-11-06 10:05:21 IST
Mega Limited			2025-11-07 11:50:44 IST	2025-11-07 11:50:44 IST
MEGASync			2025-11-07 11:50:41 IST	2025-11-07 11:50:41 IST
Microsoft			2025-11-07 12:29:44 IST	2025-11-07 12:29:44 IST
Packages			2025-11-07 12:31:43 IST	2025-11-07 12:31:43 IST

Figure 60 : Mega sync folder

MegaSync folder where all the data are store in the cloud.

megasync.lock			2025-11-07 11:50:44 IST
megasync.show			2025-11-07 12:07:47 IST
megasync.version	0		2025-11-07 12:07:46 IST

Figure 61 : Mega version file

File	Size	Last Modified	Last Accessed	Created	Modified
mega.gtxworker.cest52bc-79/9-4e3/-ad80-24aydyk	0	2025-11-07 12:55:49 IST	2025-11-07 12:55:49 IST	2025-11-07 12:55:49 IST	2025-11-07 12:55:49 IST
MEGASync.log	0	2025-11-07 12:55:47 IST	2025-11-07 12:55:47 IST	2025-11-07 12:55:47 IST	2025-11-07 12:55:47 IST

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 24 Page ← → Matches on page: - of - Match ← → 100% Θ + Reset

```
----- program start -----
11/07-06:20:44.685283 4368 DBG Windows 10 Version 2009
11/07-06:20:44.685339 4368 DBG Screen detected: \\.\DISPLAY1, 1718, 880, 96, 1
11/07-06:20:44.685340 4368 DBG Scaling not needed.
11/07-06:20:44.901735 4368 DBG Getting Local Storage key. Sid length: 28
11/07-06:20:44.903725 4368 DBG Qt Debug: false
11/07-06:20:44.903730 4368 DBG Qt Context: default 2
11/07-06:20:44.926838 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGASync/Resources_common.rcc
11/07-06:20:44.926903 4368 DBG Qt Debug: false
11/07-06:20:44.926912 4368 DBG Qt Context: default 2
11/07-06:20:44.936136 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGASync/Resources_qml.rcc
11/07-06:20:44.936187 4368 DBG Qt Debug: false
11/07-06:20:44.936192 4368 DBG Qt Context: default 2
11/07-06:20:44.940785 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGASync/qml.rcc
11/07-06:20:44.940829 4368 DBG Qt Debug: false
11/07-06:20:44.940832 4368 DBG Qt Context: default 2
11/07-06:20:44.948083 4368 DBG Registered resource file: C:/Users/MEGA/AppData/Local/MEGASync/Resources_light.rcc
11/07-06:20:45.281392 4368 DBG libuv version: 1.49.2 [megaapi_impl.cpp:6931]
11/07-06:20:45.286566 8472 ERR Could not open pipe. Error Code=2 The system cannot find the file specified. [comms_client.cpp:50]
11/07-06:20:45.286726 8472 ERR runShutdown Couldn't connect [client.cpp:53]
11/07-06:20:45.286735 8472 DBG Process::Process("C:/Users/MEGA/AppData/Local/MEGASync/mega-desktop-app-gfxworker.exe" -n=cecf52bcogs...) [process.cpp:68]
```

Figure 62 : Log files

SOFTWARE	4	SchedulingAgent	2019-12-07 09:17:28 IST	Windows 10 Mega.vmdk
SOFTWARE	4	WIC	2019-12-07 09:17:28 IST	Windows 10 Mega.vmdk
SOFTWARE	0	MEGASync v.	2025-11-07 06:20:41 IST	Windows 10 Mega.vmdk
SOFTWARE	4	Microsoft Edge Update v.1.3.2075	2025-11-06 18:01:46 IST	Windows 10 Mega.vmdk

Figure 63 : Successfully installed cloud program

Source Name	S	C	O	Path	Date Accessed	Data Source
hindsight.lnk				C:\Users\MEGA\Downloads\hindsight	2025-11-07 12:15:17 IST	Windows 10 Mega.vmdk
hindsight_gui.lnk				C:\Users\MEGA\Downloads\hindsight\hindsight_gui.py	2025-11-07 12:15:17 IST	Windows 10 Mega.vmdk
memdump.mem.lnk				C:\Users\MEGA\Desktop\memdump.mem	2025-11-07 12:43:07 IST	Windows 10 Mega.vmdk
ms-gamingoverlay---.lnk				No preferred path found	2025-11-07 12:07:27 IST	Windows 10 Mega.vmdk
ms-gamingoverlay--kglcheck-.lnk				No preferred path found	2025-11-06 12:00:31 IST	Windows 10 Mega.vmdk
setup.lnk				C:\Users\MEGA\Downloads\hindsight\setup.py	2025-11-07 12:20:32 IST	Windows 10 Mega.vmdk
TheInternet.lnk				No preferred path found	2025-11-06 12:00:31 IST	Windows 10 Mega.vmdk
setup.py.lnk				C:\Users\MEGA\Downloads\hindsight\setup.py	0000-00-00 00:00:00	Windows 10 Mega.vmdk
No preferred path found.lnk				No preferred path found	0000-00-00 00:00:00	Windows 10 Mega.vmdk
hindsight_gui.py.lnk				C:\Users\MEGA\Downloads\hindsight\hindsight_gui.py	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Pictures.lnk				C:\Users\MEGA\Pictures	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Videos.lnk				C:\Users\MEGA\Videos	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Music.lnk				C:\Users\MEGA\Music	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Downloads.lnk				C:\Users\MEGA\Downloads	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Documents.lnk				C:\Users\MEGA\Documents	0000-00-00 00:00:00	Windows 10 Mega.vmdk
Desktop.lnk				C:\Users\MEGA\Desktop	0000-00-00 00:00:00	Windows 10 Mega.vmdk

Figure 64 : All file converted in .lnk which are synced

In the software installation we can find the mega cloud client app installed in the PC.

13.4 Browser artifacts

Source Name	S	C	O	Path	URL
History			4	C:\Users\MEGA\Downloads\ChromeSetup.exe	https://dl.google.com/tag/s/appguid%3D%7B8A69D3...
History			1	C:\Users\MEGA\Downloads\MEGAsyncSetup64.exe	https://mega.nz/MEGAsyncSetup64.exe
History			4	C:\Users\MEGA\Downloads\Git-2.51.2-64-bit.exe	https://github.com/git-for-windows/git/releases/dow...
History			3	C:\Users\MEGA\Downloads\Git-2.51.2-64-bit.exe	https://release-assets.githubusercontent.com/github-...
History				C:\Users\MEGA\Downloads\Hindsight Report (2025-1...	http://localhost:8080/xlsx
KnownGameList.bin:Zone.				/Users/MEGA/AppData/Local/Microsoft/GameDVR/K...	

Figure 65 : Browser history

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Category
MEGAsync.exe				File	Likely Notable		Cloud Storage		MEGAsync

Figure 66 : Mega cloud .exe

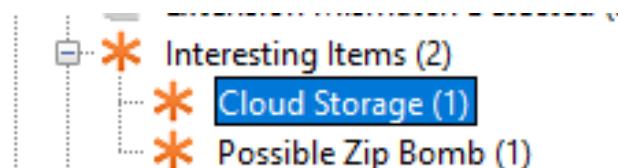


Figure 67 : Autopsy themself create cloud storage separated

Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	Program Name	Data Source
Login Data				https://mega.nz/	2025-11-07 11:49:27 IST	mega.nz	Default	https://mega.nz/	mega.nz	Microsoft Edge	Windows 10 Mega.vmdk
Login Data				https://mega.nz/	2025-11-07 11:49:27 IST	mega.nz	Person 1	https://mega.nz/	mega.nz	Google Chrome	Windows 10 Mega.vmdk

Figure 68 : mega login details

Type	Value	Source(s)
URL	https://mega.nz/	Recent Activity
Date Created	2025-11-07 11:49:27 IST	Recent Activity
Decoded URL	mega.nz	Recent Activity
Username		Recent Activity
Realm	https://mega.nz/	Recent Activity
Domain	mega.nz	Recent Activity
Program Name	Microsoft Edge	Recent Activity
Username	Default	Recent Activity
Source File Path	/img_Windows 10 Mega.vmdk/vol_vol6/Users/MEGA/AppData/Local/Microsoft/Edge/User Data/Default/Login Data	
Artifact ID	-9223372036854775595	

Figure 69 : Recent activity of login mega cloud

History		0	2025-11-07 12:41:52 IST	2025-11-07 12:41:52 IST	2025-1
History-journal			2025-11-07 12:41:52 IST	2025-11-07 12:41:52 IST	2025-1
LOCK			2025-11-07 11:47:43 IST	2025-11-07 11:47:43 IST	2025-1
LOG			2025-11-07 12:21:37 IST	2025-11-07 12:21:37 IST	2025-1
LOG.old			2025-11-07 12:15:35 IST	2025-11-07 12:21:37 IST	2025-1
Login Data	▼	0	2025-11-07 11:49:27 IST	2025-11-07 11:49:27 IST	2025-1
Login Data For Account	▼	4	2025-11-07 11:47:34 IST	2025-11-07 11:47:34 IST	2025-1
Login Data For Account-journal	▼		2025-11-07 11:47:34 IST	2025-11-07 11:47:34 IST	2025-1
Login Data-journal	▼		2025-11-07 11:49:27 IST	2025-11-07 11:49:27 IST	2025-1
			2025-11-07 12:22:06 IST	2025-11-07 12:22:06 IST	2025-1

Figure 70 : Login DATA files

Login data history.

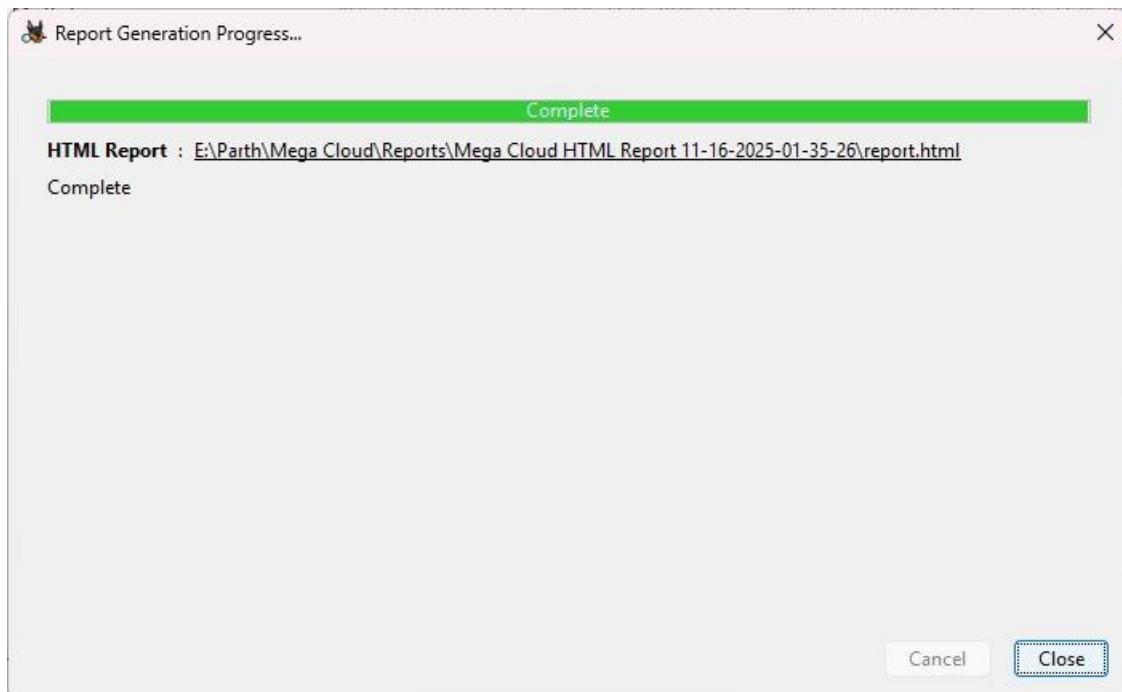


Figure 71: Report make from autopsy successfully

After successfully find all the data and evidence from the cloud drive done it by book mark we can create a report.

13.5 Live browser artifact

url	2025-11-06 22:18:06.098	https://www.google.com/search?q=mega&oq=mega&gs_lcrp=EgZjat mega - Google Search	
url	2025-11-06 22:18:06.622	https://www.google.com/search?q=mega&oq=mega&gs_lcrp=EgZjat mega - Google Search	
url	2025-11-06 22:18:09.062	https://mega.io/ MEGA: Protect your Online Privacy	
url	2025-11-06 22:18:15.316	https://mega.nz/register Create Your Account - MEGA	
autofill	2025-11-06 22:18:46.000		register-name2 Parth
autofill	2025-11-06 22:18:46.000		register-familyname2 Gondaliya
url	2025-11-06 22:18:46.686	https://mega.nz/login Login - MEGA	
autofill	2025-11-06 22:19:23.000		login-name2 gondaliyaparth076.csv@gmail.com
url	2025-11-06 22:19:23.233	https://mega.nz/fm MEGA	
login (never save)	2025-11-06 22:19:27.886	https://mega.nz/	
url	2025-11-06 22:19:27.910	https://mega.nz/fm/uM1WnBiT MEGA	
url	2025-11-06 22:19:28.399	https://mega.io/webclient/loggedin.html	
url	2025-11-06 22:19:49.282	https://www.google.com/search?q=mega&oq=&gs_lcrp=EgZjaHJvbW mega - Google Search	
site setting (hsts)	2025-11-06 22:19:50.019	Encoded domain: EUee8fEWEJXzg9tS5msiIFKED/eSKlh6OyfshJAx5qc-HSTS observed	('expiry': 1794032390.019265, 'host': 'EUee8fEWE
url	2025-11-06 22:19:52.181	https://mega.nz/desktop	MEGA Desktop App: Windows, Mac and Linux

Figure 72 : hindsight browser history by timeline

```

engagement [in Prefere {'last_modified': '13406971766548792', 'setting': {'lastEngagementTime':
profile_path C:\Users\MEGA\AppData\Local\Google\Chrome\User Data
cache_path (optional - only needed if outside of the profile path)
log_path hindsight.log
temp_dir hindsight-temp
: 500 Internal Server Error

```

Figure 73 : hindsight browser history find

14. One drive

14.1 installation process

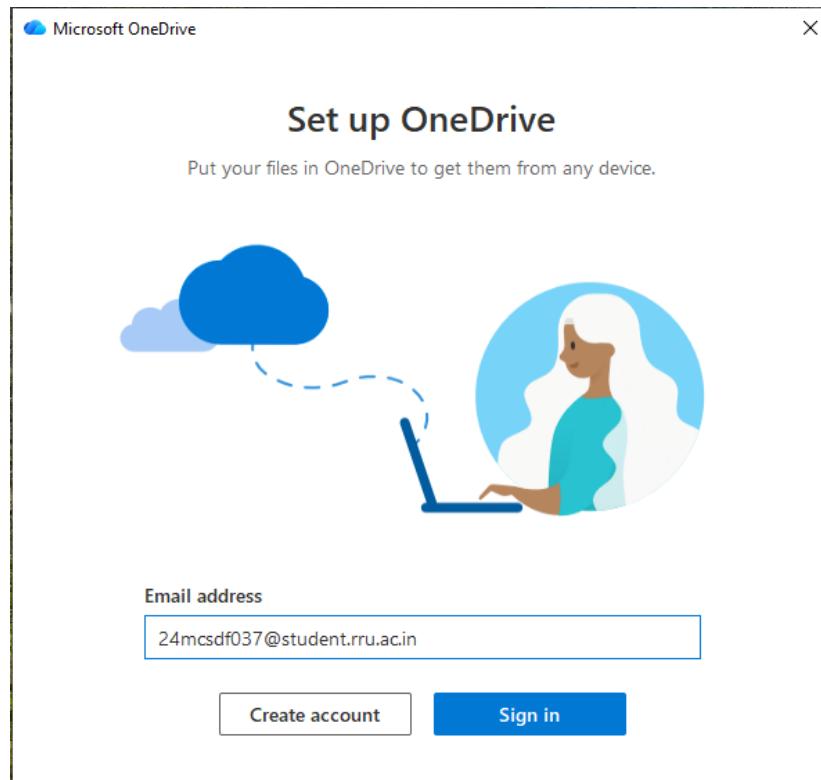


Figure 74 : installation steps

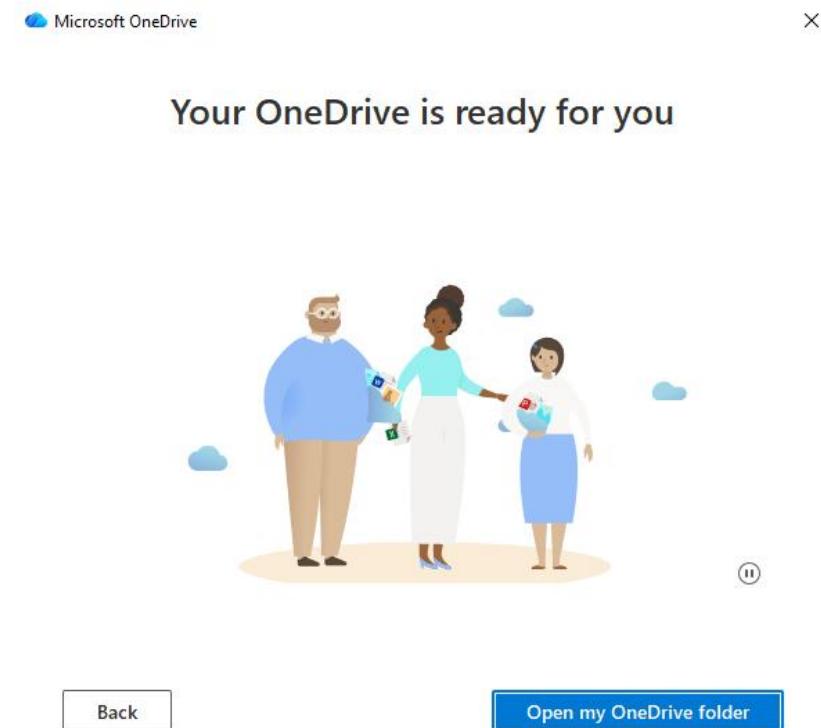


Figure 75 : successfully installed

One drive not required any installation process it is By default instated in every windows so we just enable it so that RegShot is not in use in this installation.

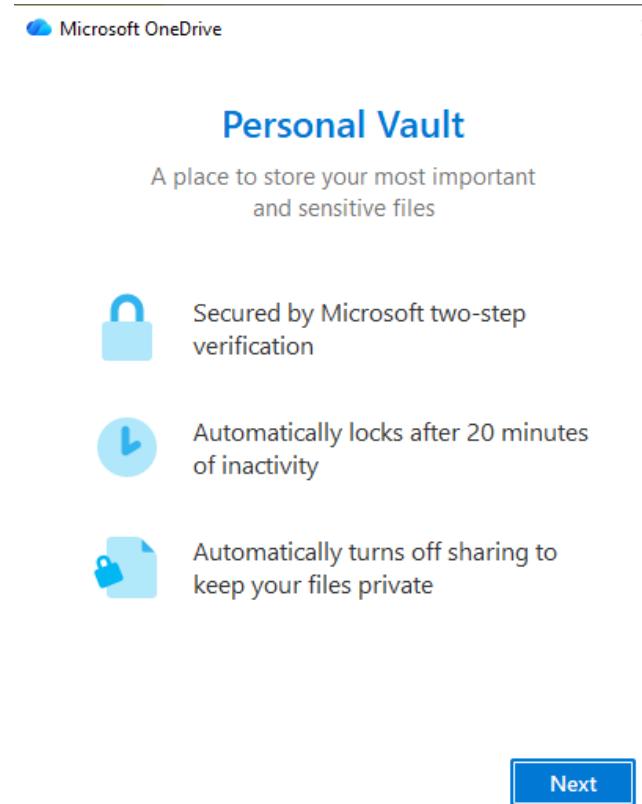


Figure 76 : Personal vault setup

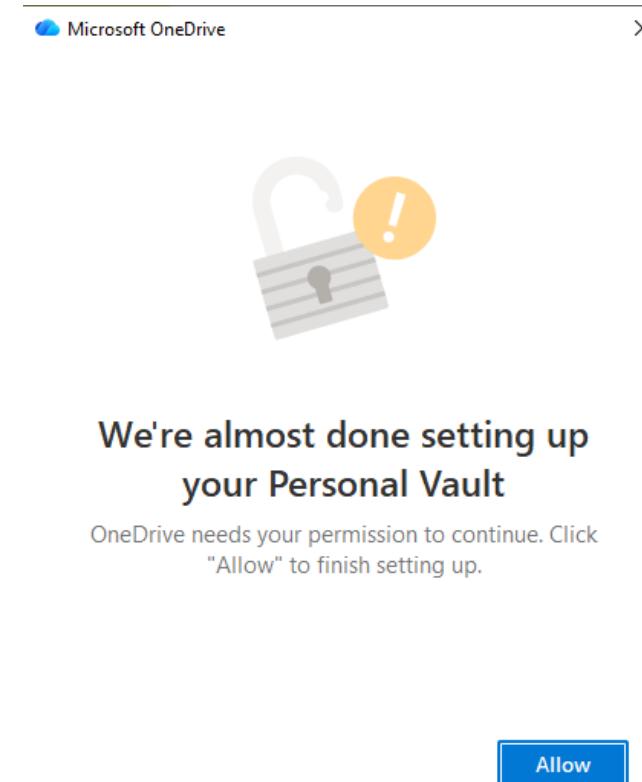


Figure 77 : Personal vault setup

My files				
	Name ↑ ▾	Modified	File size	Sharing
	Desktop	3 minutes ago	2.55 GB	Private
	Documents	10 minutes ago		Private
	Personal Vault	10 minutes ago	2.27 MB	Private
	Pictures	46 minutes ago	2.94 MB	Private
	Getting started with OneDrive.pdf	About an hour ago	1.10 MB	Private

Figure 78 : Sync folder list

One drive contacts the important folder in the windows like Desktop, Documents, Picture, and one drive is also provide the personal vault for the store the personal data in the drive.

	Name	Status
	Desktop	
	Documents	
	Pictures	
	Getting started with OneDrive	
	Personal Vault	

Figure 79 : sync status

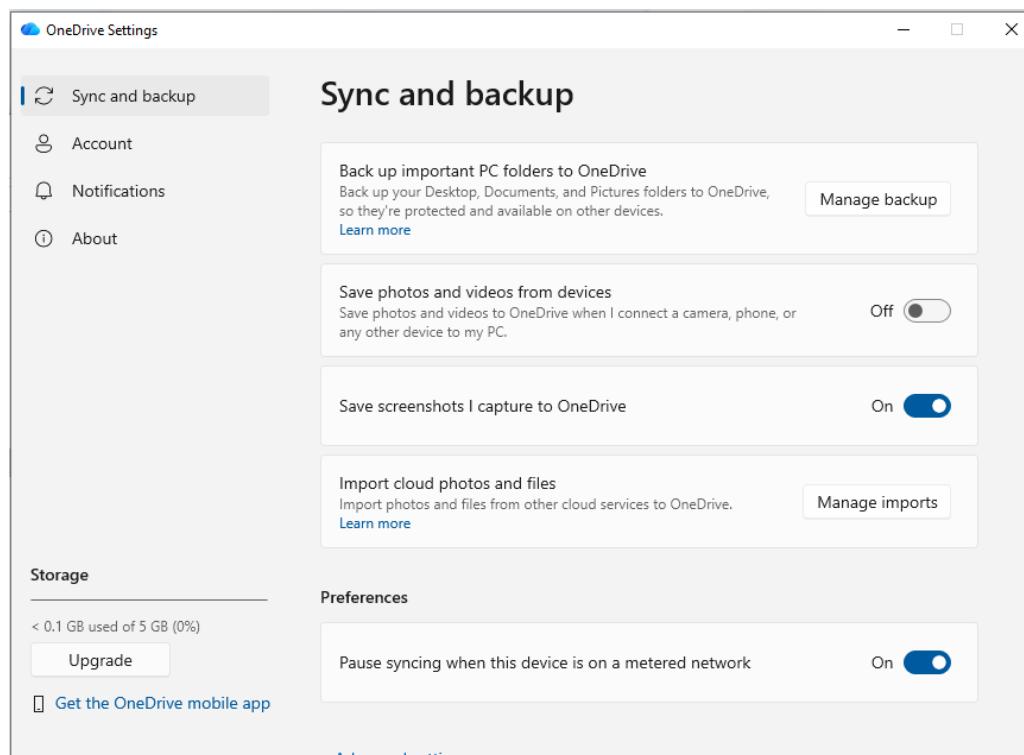


Figure 80 : Sync and backup folder setting

One drive given a 5GB storage free signup and there are also be the paid service also for the more extra space in OneDrive.

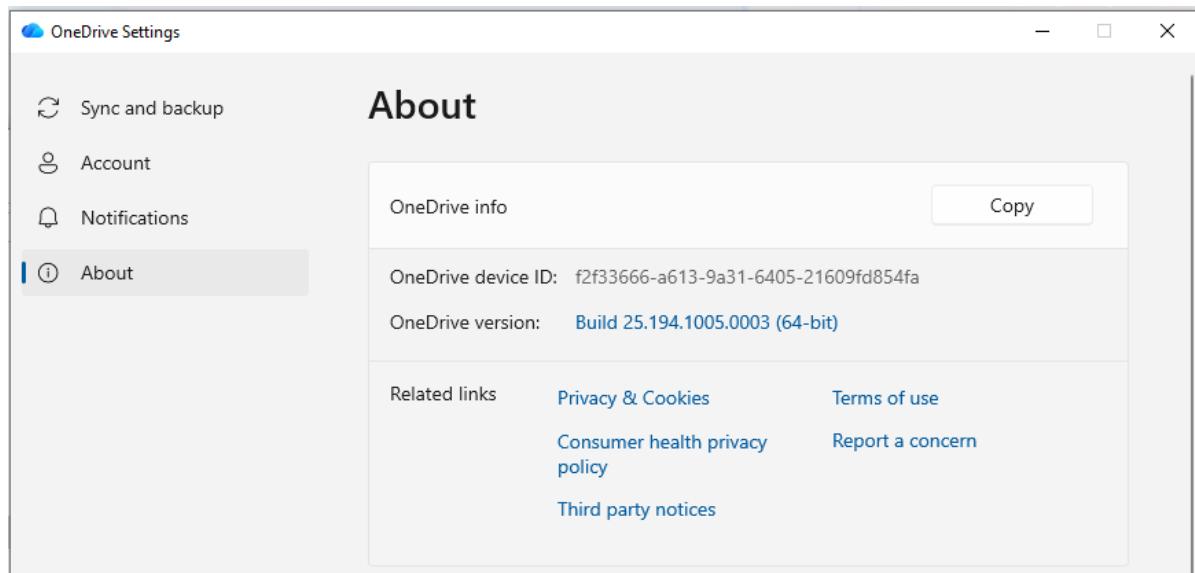


Figure 81 : Version of the one drive

OneDrive version is shown in about section.

14.2 RAM dump

0c39cb30	1d	f9	ac	00	00	00	fb	00	00	00	01	00	00	00	00	0c	00	.ù~...û.....
0c39cb40	00	00	1f	49	73	52	6f	61	6d	69	6e	67	45	6e	63	72		...IsRoamingEncr
0c39cb50	79	70	74	69	6f	6e	4b	65	79	41	76	61	69	6c	61	62		yptionKeyAvailab
0c39cb60	6c	65	00	00	00	0c	00	00	00	04	74	72	75	65	00	00		le.....true..
0c39cb70	00	0c	00	00	00	09	46	69	72	73	74	4e	61	6d	65	00	FirstName..
0c39cb80	00	00	0c	00	00	00	05	50	61	72	74	68	00	00	00	0c	Parth....
0c39cb90	00	00	00	08	55	73	65	72	4e	61	6d	65	00	00	00	0c	UserName....
0c39cba0	00	00	00	1c	32	34	6d	63	73	64	66	30	33	37	40	73	24mc sdf037@s
0c39cbb0	74	75	64	65	6e	74	2e	72	72	75	2e	61	63	2e	69	6e		tudent.rru.ac.in
0c39cbc0	00	00	00	0c	00	00	00	08	4c	61	73	74	4e	61	6d	65	LastName....
0c39cbd0	00	00	00	0c	00	00	00	09	47	6f	6e	64	61	6c	69	79	Gondaliy
0c39cbe0	61	00	00	00	0c	00	00	00	03	55	49	44	00	00	00	0c		a.....UID....
0c39cbf0	00	00	00	10	30	30	30	33	34	30	30	32	39	41	44	43	000340029ADC
0c39cc00	38	35	31	35	00	00	00	0c	00	00	00	0e	53	61	66	65		8515.....Safe
0c39cc10	43	75	73	74	6f	6d	65	72	49	64	00	00	00	0c	00	00		CustomerId.....
0c39cc20	00	10	65	39	64	39	64	34	36	61	36	38	35	36	37	62		..e9d9d46a68567b
0c39cc30	62	66	00	00	00	0c	00	00	00	08	57	41	5f	53	74	61		bf.....WA_Sta
0c39cc40	74	65	00	00	00	06	00	00	00	00	00	00	00	00	00	00		te.....
0c39cc50	00	0c	00	00	00	11	57	41	5f	52	65	76	69	73	69	6f	WA_Revisio
0c39cc60	6e	4e	75	6d	62	65	72	00	00	00	0c	00	00	00	01	32		nNumber.....2
0c39cc70	00	00	00	0c	00	00	00	05	57	41	5f	49	64	00	00	00	WA_Id...
0c39cc80	0c	00	00	00	10	30	30	30	33	34	30	30	32	39	41	44	000340029AD
0c39cc90	43	38	35	31	35	00	00	00	0c	00	00	00	0a	57	41	5f		C8515.....WA_
0c39cca0	50	72	6f	76	69	65	72	00	00	04	01	00	00	02	80	00		Provier.....€.
0c39ccb0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0c39ccc0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0c39ccd0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0c39cce0	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 82 : User id Reveal Ram Dump

At the installation time it will show the user first name and last name in the ram dump also in the ram dump the user name is shown but the password is encrypted and at the sync time full file location is show in the RAM dump.

2ba90U/00	49	3d	00	00	tt	tt	tt	tt	18	00	00	04	0b	00	00	00	00	1=..yyyy.....
2ba90710	53	63	72	65	65	6e	73	68	6f	74	73	00	0e	00	00	00	00	Screenshots.....
2ba90720	58	00	00	04	50	00	00	00	43	3a	5c	55	73	65	72	73	00	X...P...C:\Users
2ba90730	5c	4f	6e	65	44	72	69	76	65	5c	4f	6e	65	44	72	69	00	\OneDrive\OneDri
2ba90740	76	65	5c	50	69	63	74	75	72	65	73	5c	53	63	72	65	00	ve\Pictures\Scre
2ba90750	65	6e	73	68	6f	74	73	5c	41	6e	6e	6f	74	61	74	69	00	shots\Annotati
2ba90760	6f	6e	20	32	30	32	35	2d	31	31	2d	30	37	20	31	35	00	on 2025-11-07 15
2ba90770	31	39	33	34	2e	70	6e	67	28	00	00	04	20	00	00	00	00	1934.png(... ...
2ba90780	41	6e	6e	6f	74	61	74	69	6f	6e	20	32	30	32	35	2d	00	Annotation 2025-
2ba90790	31	31	2d	30	37	20	31	35	31	39	33	34	2e	70	6e	67	00	11-07 151934.png
2ba907a0	18	00	00	04	0e	00	00	00	55	70	6c	6f	61	64	65	64	00Uploaded
2ba907b0	20	74	6f	20	25	25	72	00	48	00	00	0f	0a	00	00	00	00	to %R.H.....
2ba907c0	22	97	24	01	0a	97	24	01	f2	52	a7	00	fa	5e	8b	00	00	"\$...\$.ør§.ú^<.
2ba907d0	00	00	24	01	b4	00	00	00	16	00	00	00	00	00	00	00	00	é 055

Figure 83 : Sync File Location reveal in ram dump

155	35.039232	192.168.11.132	216.58.203.35	TLSv1.3	1825 Client Hello (SNI=clientservices.googleapis.com)
179	35.057028	192.168.11.132	142.250.77.36	QUIC	1292 Initial, DCID=3448c590eec8c5d3, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO
180	35.057087	192.168.11.132	142.250.77.36	QUIC	1292 Initial, DCID=3448c590eec8c5d3, PKN: 2, PADDING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PING, PADDING, CRYPTO, PING
182	35.057432	192.168.11.132	142.250.77.36	QUIC	1292 Initial, DCID=a4b9b51be0baf633, PKN: 2, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PING, PADDING, CRYPTO, PING
194	35.068902	192.168.11.132	142.250.77.36	TLSv1.3	1810 Client Hello (SNI=www.google.com)
195	35.069549	216.58.203.35	192.168.11.132	TLSv1.3	1514 Server Hello, Change Cipher Spec
199	35.069549	216.58.203.35	192.168.11.132	TLSv1.3	116 Application Data

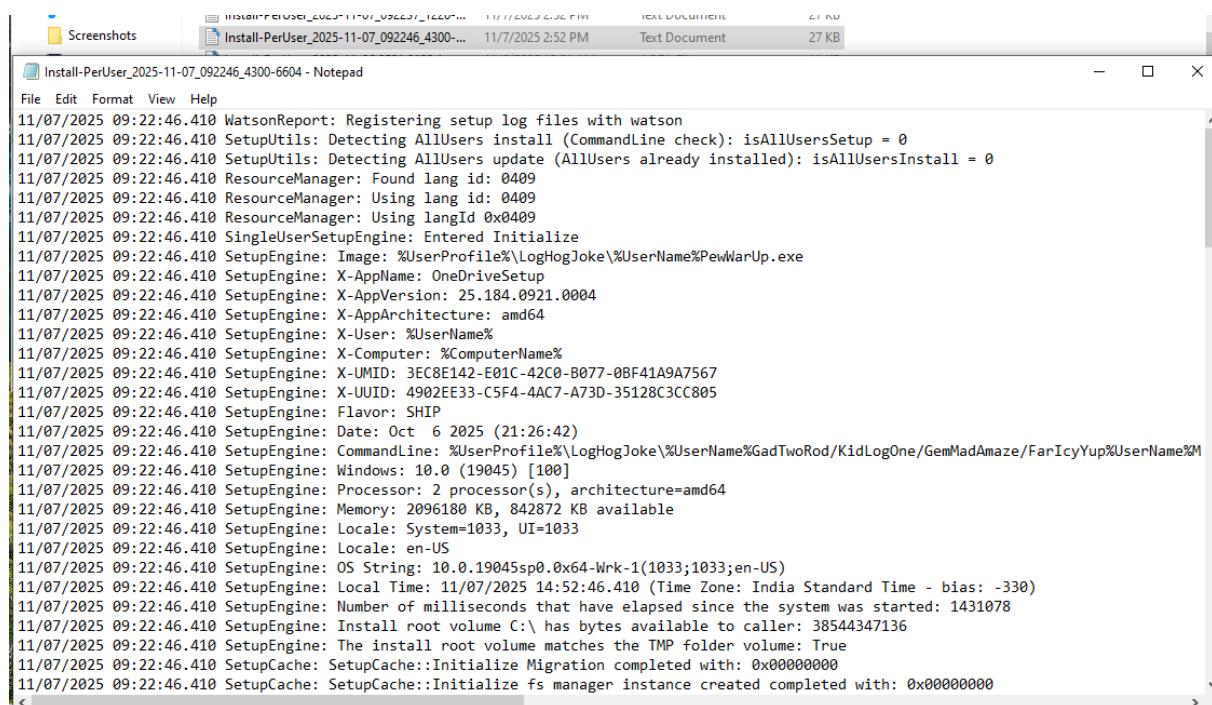
Figure 84 : Encrypted hand shake

Setup log file in the plain text.

File	Home	Share	View	Logs
← → ↻ ↺	📁	📅	📁	logs
File	Home	Share	View	
Logs	This PC	Local Disk (C:)	Users	OneDrive > AppData > Local > Microsoft > OneDrive > setup > logs
Name	Date modified	Type	Size	
DeviceHealthSummaryConfiguration	11/6/2025 10:51 AM	Configuration sett...	1 KB	
Install_2025-11-06_052144_4424-7228	11/6/2025 10:51 AM	Text Document	35 KB	
Install_2025-11-07_073133_6732-5648	11/7/2025 1:01 PM	Text Document	43 KB	
Install_2025-11-07_073147_6084-5680	11/7/2025 1:01 PM	Text Document	6 KB	
Install_2025-11-07_090419_4396-6876	11/7/2025 2:34 PM	Text Document	10 KB	
Install_2025-11-07_092136_3928-7148	11/7/2025 2:51 PM	Text Document	3 KB	
Install_2025-11-07_092141_9060-9848	11/7/2025 2:51 PM	Text Document	10 KB	
Install_2025-11-07_092236_3912-7060	11/7/2025 2:52 PM	Text Document	43 KB	
Install_2025-11-07_092245_9676-8648	11/7/2025 2:52 PM	Text Document	42 KB	
Install_2025-11-07_092754_6360-7948	11/7/2025 2:58 PM	Text Document	10 KB	
Install_2025-11-07_092923_5980-1336	11/7/2025 2:59 PM	Text Document	10 KB	
Install_2025-11-07_093325_4360-5304	11/7/2025 3:03 PM	Text Document	10 KB	
Install_2025-11-07_094611_9728-4396	11/7/2025 3:16 PM	Text Document	0 KB	
Install-2025-11-06.0521.4424.1.odl	11/6/2025 10:51 AM	AODL File	7 KB	
Install-2025-11-06.0521.4424.1.odl	11/6/2025 10:51 AM	ODL File	20 KB	
Install-2025-11-06.0521.7992.1.odl	11/6/2025 10:51 AM	ODL File	6 KB	
Install-2025-11-07.0731.6732.1.odl	11/7/2025 1:01 PM	AODL File	20 KB	

Figure 85 : 9Log Files

Sync log file in the plain text with all the details file remain for the sync and file download and upload, client id (CID) , bytes of the sync , etc. all info are there in the syncdiagnostics.log file



```

File Edit Format View Help
11/07/2025 09:22:46.410 WatsonReport: Registering setup log files with watson
11/07/2025 09:22:46.410 SetupUtils: Detecting AllUsers install (CommandLine check): isAllUsersSetup = 0
11/07/2025 09:22:46.410 SetupUtils: Detecting AllUsers update (AllUsers already installed): isAllUsersInstall = 0
11/07/2025 09:22:46.410 ResourceManager: Found lang id: 0409
11/07/2025 09:22:46.410 ResourceManager: Using lang id: 0409
11/07/2025 09:22:46.410 ResourceManager: Using langId 0x0409
11/07/2025 09:22:46.410 SingleUserSetupEngine: Entered Initialize
11/07/2025 09:22:46.410 SetupEngine: Image: %UserProfile%\LogHogJoke\%UserName%PewWarUp.exe
11/07/2025 09:22:46.410 SetupEngine: X-AppName: OneDriveSetup
11/07/2025 09:22:46.410 SetupEngine: X-AppVersion: 25.184.0921.0004
11/07/2025 09:22:46.410 SetupEngine: X-AppArchitecture: amd64
11/07/2025 09:22:46.410 SetupEngine: X-User: %UserName%
11/07/2025 09:22:46.410 SetupEngine: X-Computer: %ComputerName%
11/07/2025 09:22:46.410 SetupEngine: X-UMID: 3EC8E142-E01C-4C20-B077-0BF41A9A7567
11/07/2025 09:22:46.410 SetupEngine: X-UUID: 4902EE33-C5F4-4AC7-A73D-35128C3CC805
11/07/2025 09:22:46.410 SetupEngine: Flavor: SHIP
11/07/2025 09:22:46.410 SetupEngine: Date: Oct 6 2025 (21:26:42)
11/07/2025 09:22:46.410 SetupEngine: Commandline: %UserProfile%\LogHogJoke\%UserName%GadTwoRod/KidLogOne/GemMadAmaze/FarIcyYup%UserName%M
11/07/2025 09:22:46.410 SetupEngine: Windows: 10.0 (19045) [100]
11/07/2025 09:22:46.410 SetupEngine: Processor: 2 processor(s), architecture=amd64
11/07/2025 09:22:46.410 SetupEngine: Memory: 2096180 KB, 842872 KB available
11/07/2025 09:22:46.410 SetupEngine: Locale: System=1033, UI=1033
11/07/2025 09:22:46.410 SetupEngine: Locale: en-US
11/07/2025 09:22:46.410 SetupEngine: OS String: 10.0.19045sp0.0x64-Wrk-1(1033;1033;en-US)
11/07/2025 09:22:46.410 SetupEngine: Local Time: 11/07/2025 14:52:46.410 (Time Zone: India Standard Time - bias: -330)
11/07/2025 09:22:46.410 SetupEngine: Number of milliseconds that have elapsed since the system was started: 1431078
11/07/2025 09:22:46.410 SetupEngine: Install root volume C:\ has bytes available to caller: 38544347136
11/07/2025 09:22:46.410 SetupEngine: The install root volume matches the TMP folder volume: True
11/07/2025 09:22:46.410 SetupCache: SetupCache::Initialize Migration completed with: 0x00000000
11/07/2025 09:22:46.410 SetupCache: SetupCache::Initialize fs manager instance created completed with: 0x00000000

```

Figure 86 : Log File show in plain text

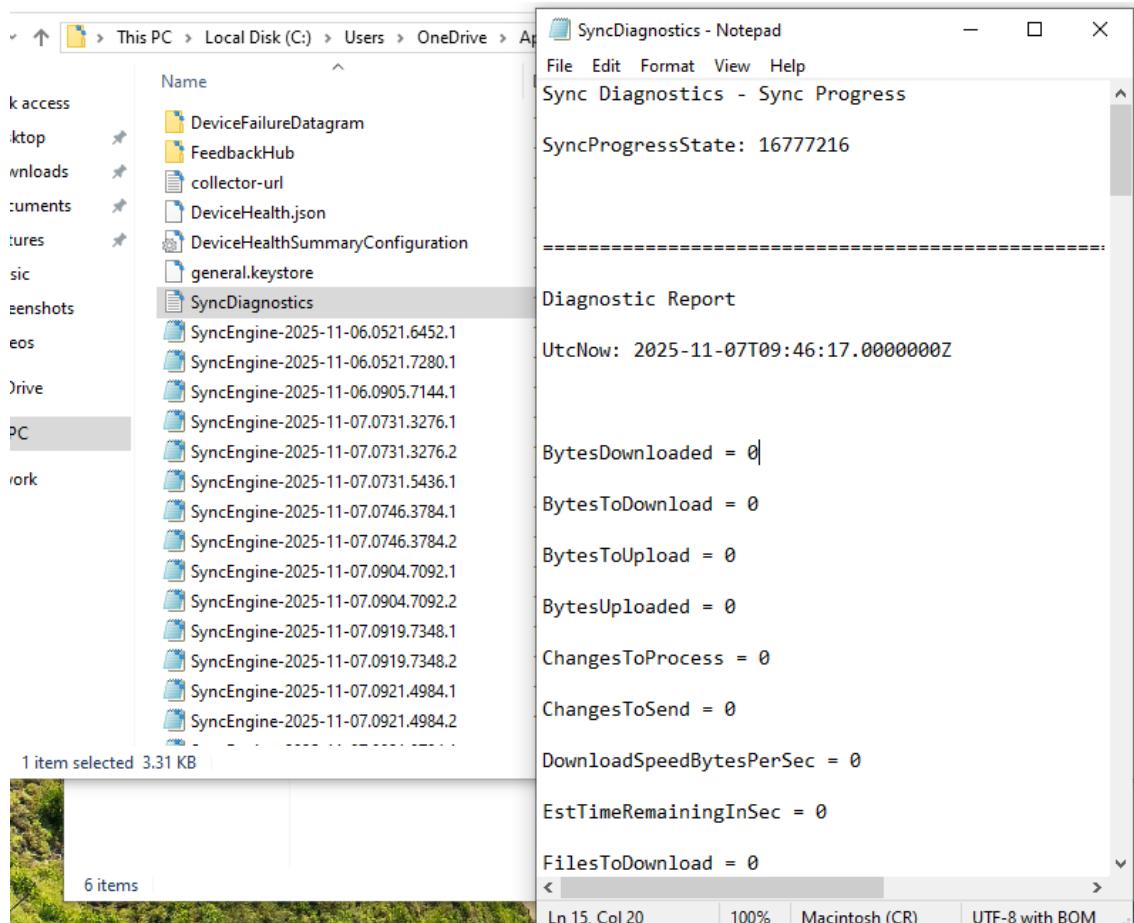


Figure87 : SyncDiagnostics.log for track all thinks

OneDrive also holds the info of the device also in plain text with the version and the last report time in plain text.

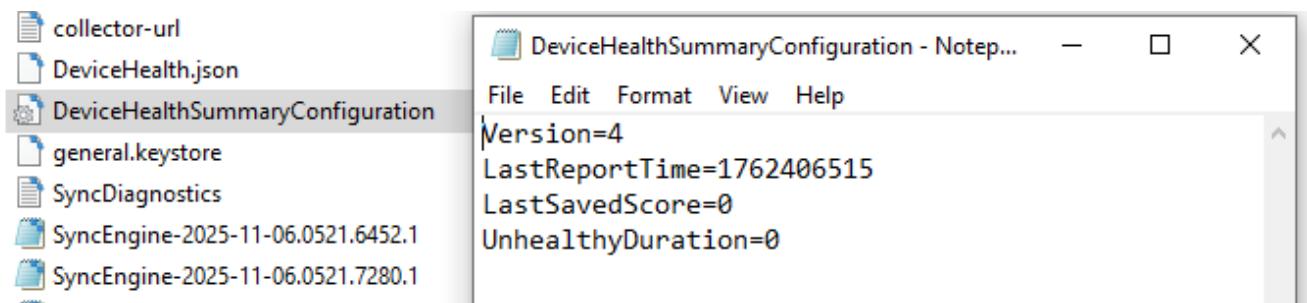


Figure 88 : Device health summary track

14.3 Disk creation

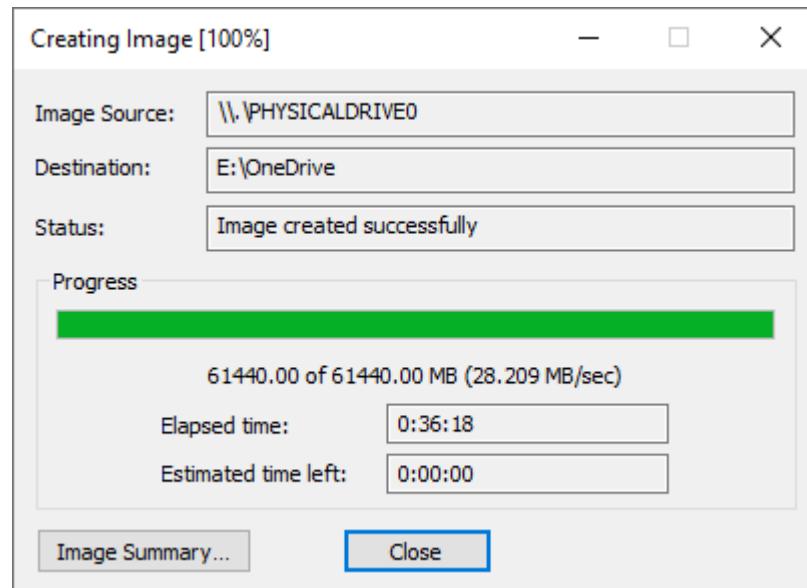


Figure 89 : image creation

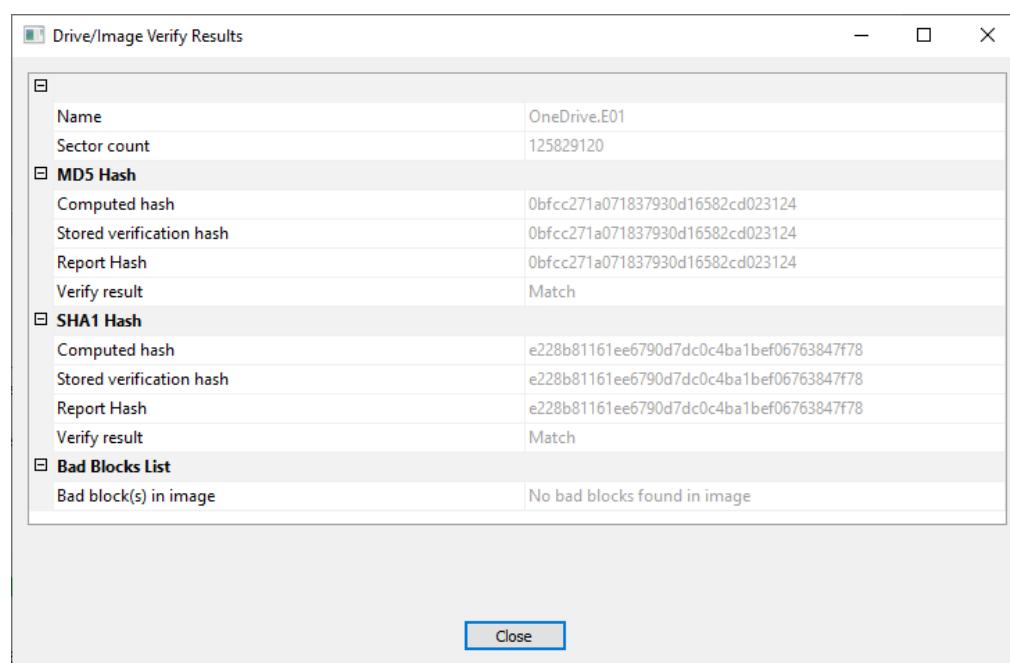


Figure 90 : successfully created image

14.4 Disk analysis

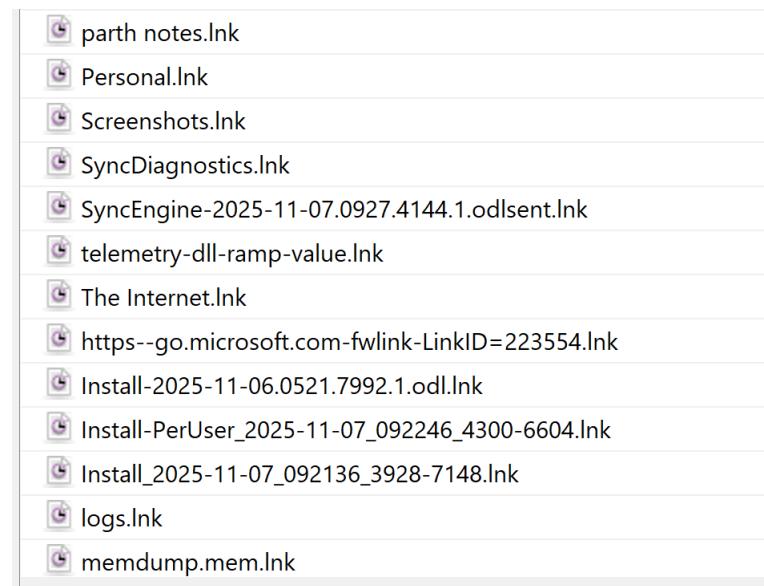


Figure 91 : 10 all files in .lnk

Type	Value	Source(s)
Path	C:\Users\OneDrive\OneDrive\Documents\parth notes.pdf	RecentActivity
Path ID	27542	RecentActivity
Date Accessed	0000-00-00 00:00	RecentActivity
Source File Path	/img_Windows 10 OneDrive.vmdk/vol_vol6/Users/OneDrive/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/5f7b5f1e01b83767.automati cDestinations-ms\parth notes.pdf.lnk	
Artifact ID	-922337203685477574	

Figure 92 : .ink file location

We can find the use of the cloud storage for the hide the doc or the make the back up of the data on the cloud storage for the make the more secret and like that we can see that there are the total 3 folder are use in the one drive of the cloud storage Desktop, Documents, Picture and setting default pdf of the OneDrive.

Name	S	C	O	Modified Time	C
[current folder]				2025-11-07 16:31:11 IST	20
[parent folder]				2025-11-07 16:30:49 IST	20
Desktop				2025-11-07 15:45:32 IST	20
Documents				2025-11-07 15:44:28 IST	20
Pictures				2025-11-07 15:14:31 IST	20
.849C9593-D756-4E56-8D6E-42412F2A707B	0			2025-11-07 16:31:11 IST	20
desktop.ini	0			2025-11-07 15:00:14 IST	20
Getting started with OneDrive.pdf	0			2025-11-07 14:51:36 IST	20
Personal Vault.lnk	0			2025-11-07 16:31:11 IST	20

Figure 93 : list of all files are in cloud

But in the one drive the features of the personal vault that vault is also be used for the put the .doc safe Desktop we can find all the files are user and deleted from the desktop.

Regshot-1.9.0
SAMPLE STUFF
blooms-113004.mp4
cat-g62b035a58_1920.jpg
desktop.ini
hd-wallpaper-g58f7e4a77_1920.jpg
hd-wallpaper-g5930fa713_1920.jpg
hd-wallpaper-g69e16c2d8_1920.jpg
Hex Editor Neo.Ink
hindsight.log
hindsight_gui - Shortcut.lnk
memdump.mem
memdump.mem:\${3D0CE612-FDEE-43f7-8ACA-957BEC}
Microsoft Edge.lnk
Microsoft Teams.lnk
One drive.docx

Figure 94 : all deleted and move files

Here the amylase is confuse that desktop is empty means that all data in the Desktop are in the cloud data that's why we cannot find the any 1 thing in the desktop.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2025-11-06 10:49:42 IST	2025-11-06 10:49:42 IST	2025-11-06 10:49:42 IST	2025-11-06 10:49:42 IST	48	Allocated	Allocated
[parent folder]				2025-11-07 16:30:49 IST	2025-11-07 16:30:49 IST	2025-11-07 16:30:49 IST	2025-11-06 10:49:42 IST	256	Allocated	Allocated

Figure 95 : Real Desktop image

logUploaderSettings_temp.ini	0	2025-11-07 16:31:20 IST	2025-11-07 16:31:20 IST
OCSI.db	0	2025-11-07 14:59:21 IST	2025-11-07 14:59:21 IST
OCSI.dbshm	0	2025-11-07 16:31:00 IST	2025-11-07 16:31:00 IST

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occur			
Table ocsi_map_paths_r...		19 entries	Page 1 of 1
parentFSID	itemName	resourceID	isFile
1407374883600151,31121544	Annotation 2025-11-07 150231.png	819cf06b1ba848e5b143968bd8bc028..	1
1407374883600151,31121544	Annotation 2025-11-07 150303.png	e54f90a7150a4b17a7f91c1f9af1ef81	1
1407374883600151,31121544	Annotation 2025-11-07 151934.png	3a188123ef314e14831649d14068b66..	1
1407374883600151,31121544	Annotation 2025-11-07 152020.png	d8b7d50357164969ad87823a229ef3a..	1
1407374883663706,31121544	Hex Editor Neo.lnk	adef8b1fa7be4cf4b620fdf3e7ec064d	1
1407374883663706,31121544	memdump.mem	79d8f8a93bae4a4c9ee9cada74ae2ede	1
3659174697285390,31121544	file capture.pcapng	c4c2a42c0e3c40ceb9d2f1f65c1e1dee	1
3659174697285390,31121544	Getting started with OneDrive.pdf	ddfd95a8f0a64c81b36c9ff459503a1b..	1
3659174697285390,31121544	hello notes.pdf	113e45b001ee4d06a62357b7c904bbf..	1
3659174697285390,31121544	parth notes.pdf	3eb3dbddd3314087b9af0a15f63c0a5..	1
3659174697285390,31121544	parth.xlsx	08fee6c2ee644c30996febe726dd4eb3..	1
844424930240214,311215444	Camera Roll	c6fc72e302b44373a4cdb23527b05bf0..	0
844424930240214,311215444	Saved Pictures	513966737c3346b3b735e838c98b61c..	0

Figure 96 : Real Desktop image

I have to find OCSI.db file. This is a OneDrive configuration and sync information database. It is a SQLite database used internally by Microsoft OneDrive to store sync metadata, account configuration, cached file information, and operational state for a users OneDrive account.

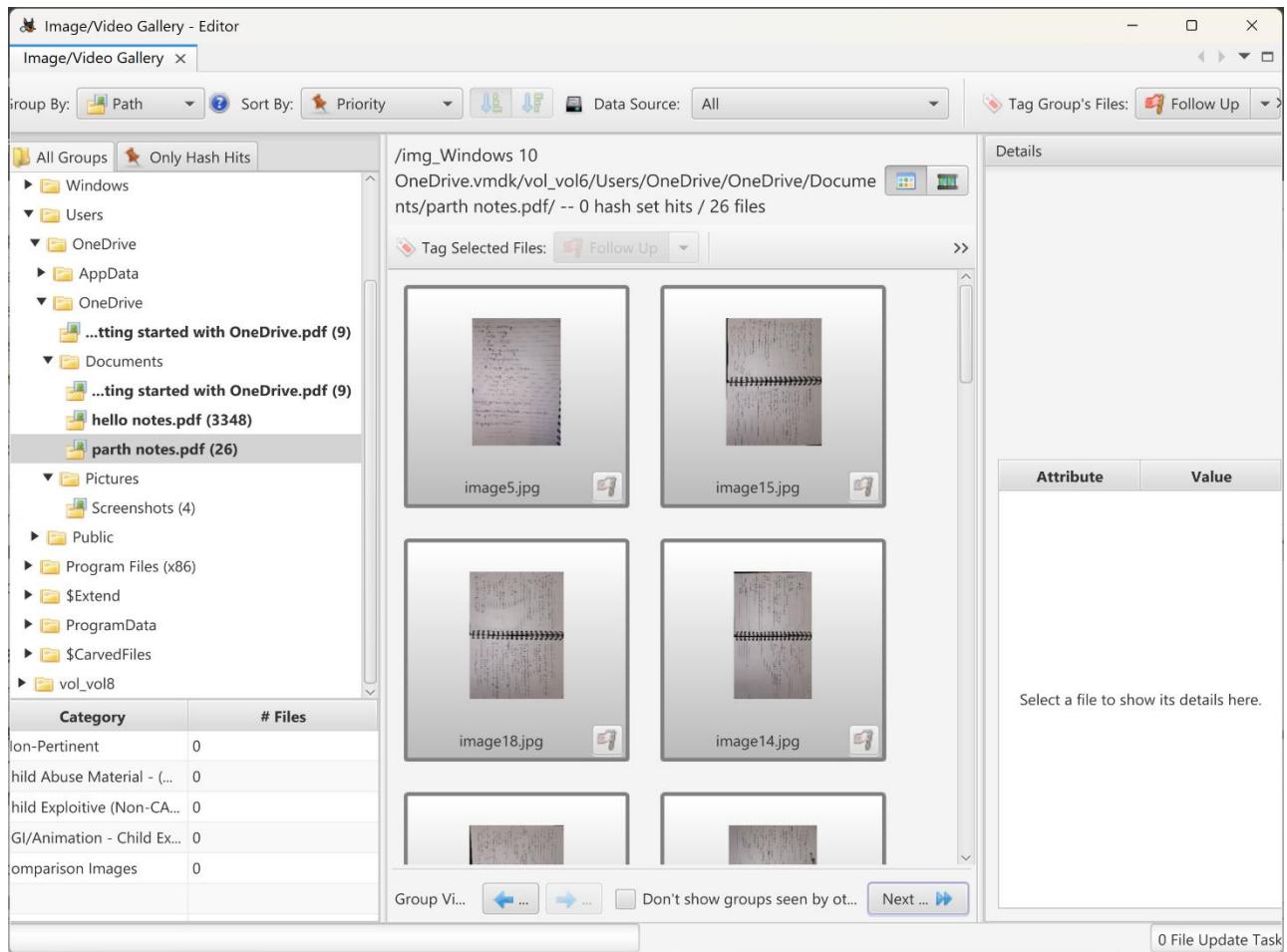


Figure 97 : Found PDF file as image

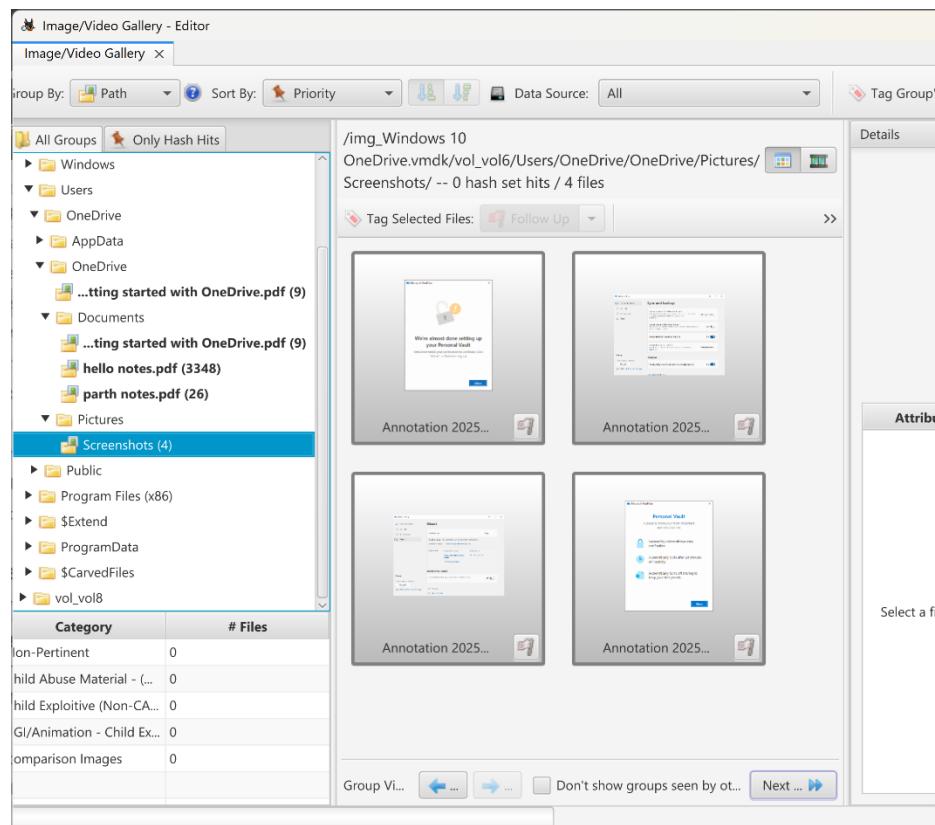


Figure 98 : screenshots found

We can find all the image are there in the drive with all screen short, pdf and other data.

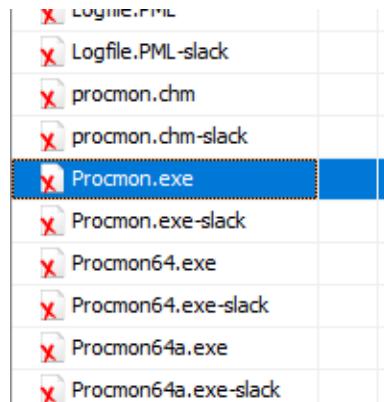


Figure 99 : files are deleted

Some software are deleted by the user after the uploaded in the one drive.

14.5 Browser artifact

Source Name	S	C	O	URL	Domain	Username
WebCacheV01.dat				odopen://unlockVault?accounttype=personal		OneDrive
WebCacheV01.dat				ms-screensketch:edit?&source=Toast&isTemporary=true&sharedAccessToken...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/OneDrive/Pictures/Screenshots/Annotation%202025-..		OneDrive
WebCacheV01.dat				ms-screensketch:edit?&source=Toast&isTemporary=true&sharedAccessToken...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/OneDrive/Pictures/Screenshots/Annotation%202025-..		OneDrive
WebCacheV01.dat				ms-screensketch:edit?&source=Toast&isTemporary=true&sharedAccessToken...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/OneDrive/Pictures/Screenshots/Annotation%202025-..		OneDrive
WebCacheV01.dat				ms-screensketch:edit?&source=Toast&isTemporary=true&sharedAccessToken...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/OneDrive/Pictures/Screenshots/Annotation%202025-..		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/setup/logs/Insta...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/setup/logs/Insta...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/setup/logs/Insta...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/logs/Personal/S...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/logs/Personal/S...		OneDrive
WebCacheV01.dat				file:///C:/Users/OneDrive/AppData/Local/Microsoft/OneDrive/logs/Personal/c...		OneDrive

Figure 100 : browser history

/img_Windows 10 OneDrive.vmdk/vol_vol6/Users/OneDrive/OneDrive/Pictures/Screenshots						
Table Thumbnail Summary						
Page: 1 of 1 Pages: ← → Go to Page: <input type="text"/>						
Name	S	C	O	Modified	Tir	
[current folder]						2025-11-07 1
[parent folder]						2025-11-07 1
Annotation 2025-11-07 150231.png	0					2025-11-07 1
Annotation 2025-11-07 150231.png:Zone.Identifier	0					2025-11-07 1
Annotation 2025-11-07 150303.png	0					2025-11-07 1
Annotation 2025-11-07 150303.png:Zone.Identifier	0					2025-11-07 1
Annotation 2025-11-07 151934.png	0					2025-11-07 1
Annotation 2025-11-07 151934.png:Zone.Identifier	0					2025-11-07 1
Annotation 2025-11-07 152020.png	0					2025-11-07 1
Annotation 2025-11-07 152020.png:Zone.Identifier	0					2025-11-07 1
desktop.ini	0					2025-11-07 1

Figure 101 : Screenshots data found

Local State	Default	000340029ADC8515	Personal	Profile 1	24mcsdf037@student.rru.ac.in	Microsoft Edge
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences						
Result: 1 of 1 Result ← →						
Type	Value					
Path	Default					
User ID	000340029ADC8515					
Domain						
Short Cut	Personal					
Name	Profile 1					
Username	24mcsdf037@student.rru.ac.in					
Program Name	Microsoft Edge					
Source File Path	/img_Windows 10 OneDrive.vmdk/vol_vol6/Users/OneDrive/AppData/Local/Microsoft/Edge/User Data/Local State					
Artifact ID	-9223372036854775628					

Figure 102 : Email ID found profile

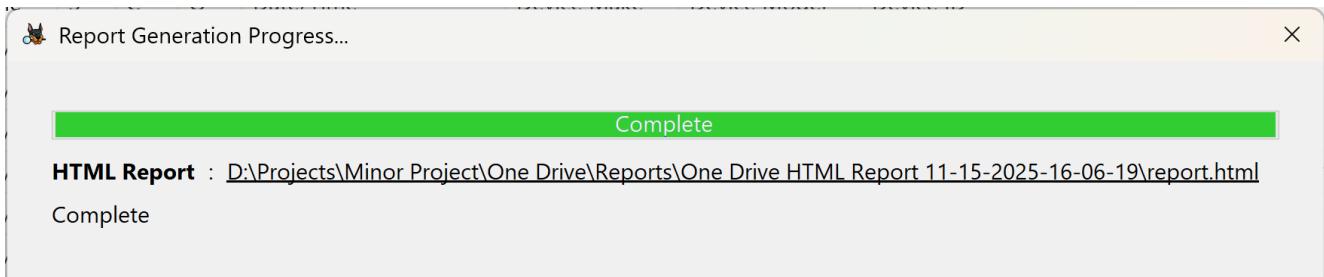


Figure 103 : created successfully report

14.6 Live browser artifact

site setting (modified 2025-11-15 03:49:40.538 https://[*].microsoft.com,*	cookie_controls_metadata [in Pr['last_modified': '1340768098053
url 2025-11-15 03:49:51.586 https://go.microsoft.com/fwlink/p/?LinkId=2119709&clcid=0x4009&culture:Continue	
url 2025-11-15 03:49:51.586 https://onedrive.live.com/about/auth?signin=1&culture=en-in&country=in	Continue
url 2025-11-15 03:49:51.586 https://onedrive.live.com/?gologin=1	Continue
url 2025-11-15 03:49:51.586 https://login.live.com/login.srf?wa=wsignin1%2E0&rpsnv=180&ct=17632073	Continue
url 2025-11-15 03:49:52.932 https://onedrive.live.com/?view=1&gologin=1	Microsoft OneDrive
site setting (modified 2025-11-15 03:49:52.934 https://[*].live.com,*	cookie_controls_metadata [in Pr['last_modified': '1340768099293
site setting (modified 2025-11-15 03:49:52.935 https://login.live.com:443,*	media_engagement [in Preferen {'expiration': '1341545699293538
url 2025-11-15 03:49:54.310 https://onedrive.live.com/?view=1	Home - OneDrive
site setting (modified 2025-11-15 03:49:54.951 https://onedrive.live.com:443,*	app_banner [in Preferences.prof ('last_modified': '1340768099495
url 2025-11-15 03:50:01.872 https://onedrive.live.com/?view=1	Home - OneDrive
url 2025-11-15 03:50:07.399 https://onedrive.live.com/?view=0	My files - OneDrive
url 2025-11-15 03:50:12.338 https://onedrive.live.com/?view=3	OneDrive
url 2025-11-15 03:50:13.532 https://onedrive.live.com/?view=3	OneDrive
url 2025-11-15 03:50:15.117 https://onedrive.live.com/?view=1	Home - OneDrive
site setting (engagemen2025-11-15 03:50:24.347 https://onedrive.live.com:443,*	lastEngagementTime in Preferen {'last_modified': '1340768102434
site setting (modified 2025-11-15 03:50:24.347 https://onedrive.live.com:443,*	site_engagement [in Preferences ('last_modified': '1340768102434
url 2025-11-15 03:50:24.563 https://onedrive.live.com/?view=0	My files - OneDrive
url 2025-11-15 03:50:26.057 https://onedrive.live.com/?view=1	Home - OneDrive
site setting (characte2025-11-15 03:50:30.000 www.microsoft.com	Status: Live last_loaded: 1763207430updates
site setting (modified 2025-11-15 03:50:30.779 https://www.microsoft.com:443,*	media_engagement [in Preferen {'expiration': '1341545703077983
site setting (characte2025-11-15 03:50:31.000 onedrive.live.com	Status: Live last_loaded: 1763207431updates
site setting (modified 2025-11-15 03:50:31.735 https://onedrive.live.com:443,*	media_engagement [in Preferen {'expiration': '1341545703173537
url 2025-11-15 03:50:36.584 http://localhost:8080/	Hindsight
site setting (modified 2025-11-15 03:50:36.586 http://localhost:*	cookie_controls_metadata [in Pr['last_modified': '1340768103658
site setting (engagemen2025-11-15 03:50:36.587 http://localhost:8080,*	lastEngagementTime in Preferen {'last_modified': '1340768103658

Figure 104 : histroy of one drive login

2025-11-15 03:42:06.434	www.microsoft.com	HSTS observed	{'expiry': 1794742926.4343, 'host': 'AVsuOZgBg0wdpKMoxm8zihjqET8kl4Xl8bCS
2025-11-15 03:42:29.000	onedrive.live.com	Status: Live	last_loaded: 1763206949
2025-11-15 03:42:31.110	https://portal.office.com/onedrive?msafed=0&wsucxt=2&username=2mc sdf Sign in to your account		
2025-11-15 03:42:31.110	https://portal.office.com/login?login_hint=2mc sdf037%40student.rru.ac.in&Sign in to your account		
2025-11-15 03:42:31.110	https://login.microsoftonline.com/common/oauth2/authorize?client_id=000 Sign in to your account		
2025-11-15 03:42:53.000			
2025-11-15 03:42:53.000	login.microsoftonline.com	Status: Live	last_loaded: 1763206973
2025-11-15 03:42:54.794	https://login.live.com:443,*	client_hints [in Preferences.profi]	{'last_modified': '13407680574794564', 'setting': {'client_hints': [14]}}
2025-11-15 03:42:54.814	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.362	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.371	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.380	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.384	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.398	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.401	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:00.404	https://login.live.com/oauth20_authorize.srf?scope=openid+profile+email+o	Enter your code	
2025-11-15 03:43:14.122	https://login.live.com/ppsecure/post.srf?mkt=en-US&username=24mc sdf03	Continue	
2025-11-15 03:43:19.000	login.live.com	Status: Live	last_loaded: 1763206999
2025-11-15 03:43:20.535	https://login.live.com/ppsecure/post.srf?mkt=en-US&username=24mc sdf03	Continue	
2025-11-15 03:43:21.466	https://login.microsoftonline.com/common/federation/oauth2msa	Working...	

Figure 105 : onedrive login id

local storage	https://onedrive.live.com	mats-telemetry-profile-id	019a8759-b611-7213-ae21-0305e438ee73
local storage	https://onedrive.live.com	migrationStoree9d9d46a68567bbf	{"version":2,"isMigrated":true}
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1-00000000-0000-0000-e9d9-d46a685{"id":"019a8759-b612-7000-94e6-627d91e064b4","nonce":	
local storage	https://onedrive.live.com	msal.1.account.keys	["msal.1-00000000-0000-0000-e9d9-d46a68567bbf.918804
local storage	https://onedrive.live.com	msal.1.token.keys.865367a6-9c28-4844-88ce-259d34dbal	{"idToken": ["msal.1-00000000-0000-0000-e9d9-d46a68567
local storage	https://onedrive.live.com	msal.865367a6-9c28-4844-88ce-259d34dbal	{"homeAccountId": "00000000-0000-0000-e9d9-d46a68567
session storage	https://onedrive.live.com/	msal.version	4.22.0
session storage	https://onedrive.live.com/	BrowserStorageTest	
session storage	https://onedrive.live.com/	BrowserStorageTest	
session storage	https://onedrive.live.com/	experimentLogCache	90343true90366true
session storage	https://onedrive.live.com/	experimentLogCacheTime	2025-11-15T11:49:53.1804327Z

Figure 106 : onedrive local and session storage

15. Google drive

15.1 Introduction to google drive:

Google Drive is a cloud-based storage service that allows users to store files online using internet, access them from anywhere, and share them easily. It was launched by Google in April 2012 and has since become one of the most popular cloud storage platforms worldwide.

As of recent data, Google Drive has over 2.6 billion active users globally, a significant increase from earlier figures. It provides 15 GB of free storage for individual users, which is shared across Google services like Gmail, Google Photos, and Google Drive itself. If you need more space, you can upgrade to one of Google One's paid plans, which offer options starting from 100 GB to 2 TB and more.

Google Drive is compatible with numerous devices, as stated below:

1. **Windows**
2. **macOS**
3. **Android**
4. **iOS**

Google Drive is a wonderful service if you want to sync, store, and share files with ease across your devices because it provides apps for desktops and mobile phones. Moreover, its close integration with other Google Workspace applications (e.g. Docs, Sheets, and Slides) turns it into a very powerful tool both for individuals and groups working together professionally.

So, whether you're backing up photos, collaborating on documents, or just storing files for safekeeping, Google Drive offers a flexible and reliable cloud storage solution.

15.2 Installation

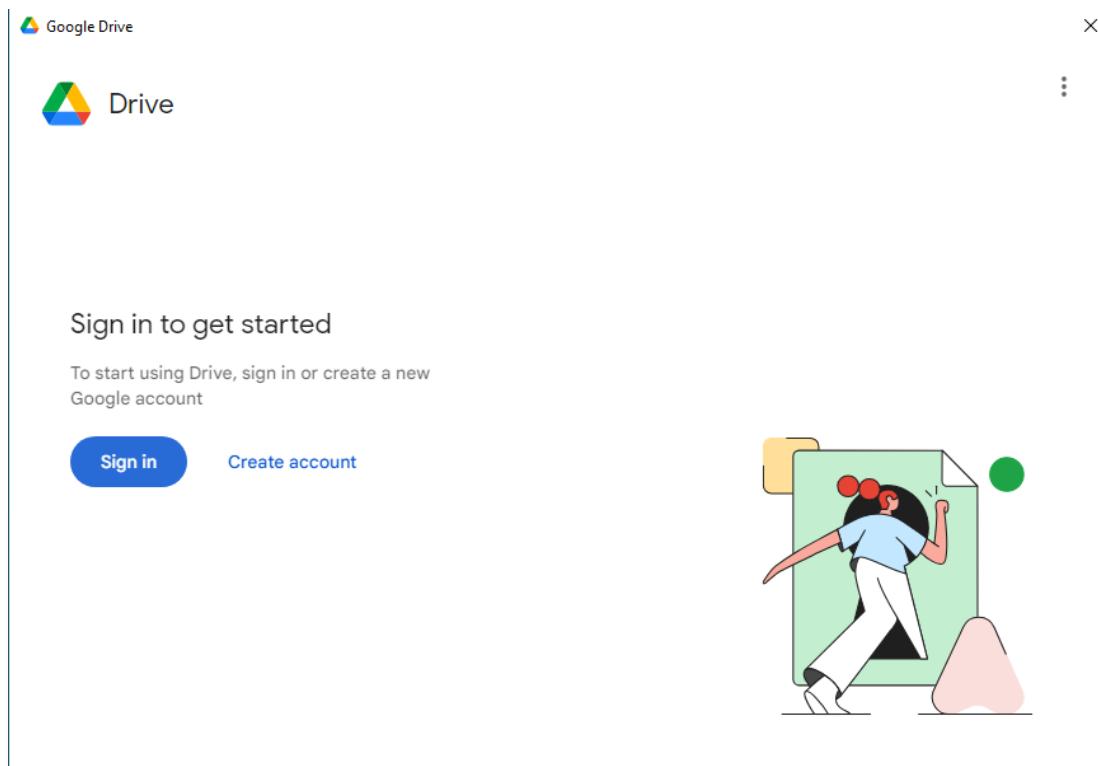


Figure 107 : Gdrive login page

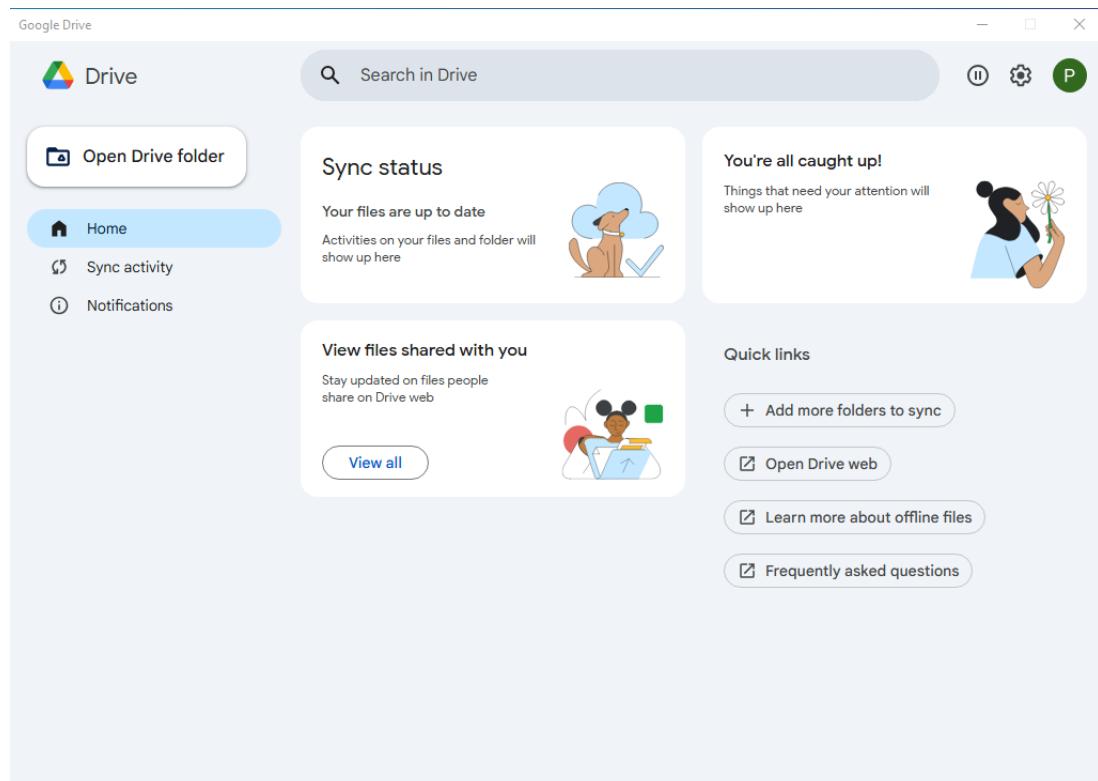


Figure 108 : Gdrive successfully installed

Google Drive is installed successfully in the local pc.

This PC > Local Disk (C:) > Program Files > Google > Drive File Stream >				
	Name	Date modified	Type	Size
	116.0.6.0	11/7/2025 4:24 PM	File folder	
	Drivers	11/7/2025 4:24 PM	File folder	
	account_export_tool	11/7/2025 4:24 PM	Application	25,708 KB
	diagnostic_tool	11/7/2025 4:24 PM	Application	25,195 KB
	docs	11/7/2025 4:24 PM	Icon	279 KB
G:	drive_fs	11/7/2025 4:24 PM	Icon	23 KB
n	launch	11/7/2025 4:24 PM	Windows Batch File	2 KB
	sheets	11/7/2025 4:24 PM	Icon	279 KB
	slides	11/7/2025 4:24 PM	Icon	279 KB

Figure 109 : Gdrive installed path

Google Drive Client installed inside the program file folder

Location “C:\Program Files\Google\Drive File Stream”

PC > Local Disk (C:) > Users > GDrive > AppData > Local > Google > DriveFS				
	Name	Date modified	Type	Size
	108365441621294550317	11/11/2025 1:58 PM	File folder	
	cef_cache	11/7/2025 4:26 PM	File folder	
	Crashpad	11/7/2025 4:25 PM	File folder	
	Logs	11/11/2025 1:58 PM	File folder	
	webview2_user_data	11/11/2025 1:58 PM	File folder	
	cello_assert_history	11/7/2025 4:26 PM	File	1 KB
	com.google.drive.nativeproxy.json	11/11/2025 1:58 PM	JSON File	1 KB
	experiments	11/11/2025 1:58 PM	Data Base File	60 KB
	first-run-info	11/7/2025 4:26 PM	File	1 KB
	global_feature_config	11/11/2025 1:58 PM	File	2 KB
	metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	12 KB
	metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
	metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
	pid	11/11/2025 1:58 PM	Text Document	1 KB
	root_preference_sqlite	11/11/2025 1:58 PM	Data Base File	36 KB
	root_preference_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
	root_preference_sqlite.db-wal	11/11/2025 1:59 PM	DB-WAL File	9 KB

Figure 110 : Gdrive DB files

Client configuration is stored in the user profile, so we have different profiles for each user in the hidden file from the location “C:\Users\GDrive\AppData\Local\Google\DriveFS”

In the updated version the user_default folder is not created instead of the drive is created an encrypted folder in number only in that folder the user data is stored.

Location is look like "C:\Users\GDrive\AppData\Local\Google\DriveFS\106807315777188389081"

Name	Date modified	Type	Size
content_cache	11/11/2025 1:58 PM	File folder	
local_folders	11/7/2025 4:25 PM	File folder	
thumbnails_cache	11/11/2025 1:58 PM	File folder	
account_settings	11/7/2025 4:26 PM	File	0 KB
case_insensitivity	11/7/2025 4:25 PM	File	0 KB
cello_experiment_token	11/11/2025 1:58 PM	File	1 KB
cello_metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	16 KB
cello_metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
cello_metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
cello_server_token	11/11/2025 1:58 PM	File	1 KB
content_cache_file_created	11/7/2025 4:26 PM	File	0 KB
core_feature_config	11/11/2025 1:58 PM	File	4 KB
enabled	11/7/2025 4:25 PM	File	0 KB
experiment_token	11/11/2025 1:58 PM	File	1 KB
identifier	11/11/2025 1:58 PM	File	1 KB
metadata_sqlite_db	11/11/2025 1:58 PM	File	472 KB
metadata_sqlite_db_local_counter_mmap	11/7/2025 4:25 PM	File	1 KB
metadata_sqlite_db-shm	11/11/2025 1:58 PM	File	32 KB
metadata_sqlite_db-vacuum_sentinel.bin	11/7/2025 4:26 PM	BIN File	1 KB
metadata_sqlite_db-wal	11/11/2025 1:58 PM	File	21 KB
metadata_update_db	11/7/2025 4:26 PM	File	28 KB
metadata_update_db-shm	11/11/2025 1:58 PM	File	32 KB
metadata_update_db-wal	11/11/2025 1:58 PM	File	0 KB
metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	24 KB
metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
mirror_cello_metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	8 KB
mirror_cello_metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
mirror_cello_metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
mirror_metadata_sqlite	11/11/2025 1:58 PM	Data Base File	156 KB
mirror_metadata_sqlite.db_local_counter...	11/7/2025 4:25 PM	DB_LOCAL_COUN...	1 KB
mirror_metadata_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB

Figure 111 : Gdrive User Data files

Some other files are also installed by the drive installation like Google slide, sheet and docs.

> This PC > Local Disk (C:) > Program Files > Google > Drive File Stream >

Name	Date modified	Type	Size
116.0.6.0	11/7/2025 4:24 PM	File folder	
Drivers	11/7/2025 4:24 PM	File folder	
account_export_tool	11/7/2025 4:24 PM	Application	25,708 KB
diagnostic_tool	11/7/2025 4:24 PM	Application	25,195 KB
docs	11/7/2025 4:24 PM	Icon	279 KB
drive_fs	11/7/2025 4:24 PM	Icon	23 KB
launch	11/7/2025 4:24 PM	Windows Batch File	2 KB
sheets	11/7/2025 4:24 PM	Icon	279 KB
slides	11/7/2025 4:24 PM	Icon	279 KB

Figure 112 : Other files are also installed by GDrive

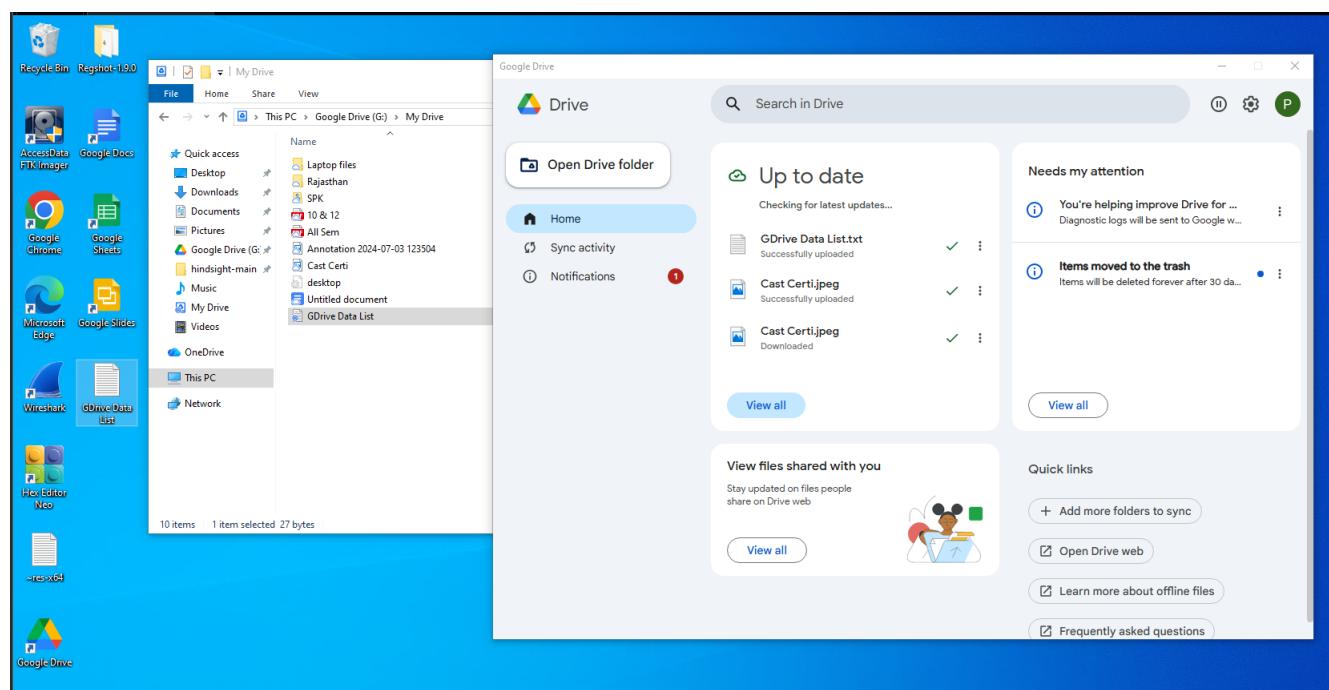


Figure 113 : Gdrive local Disk

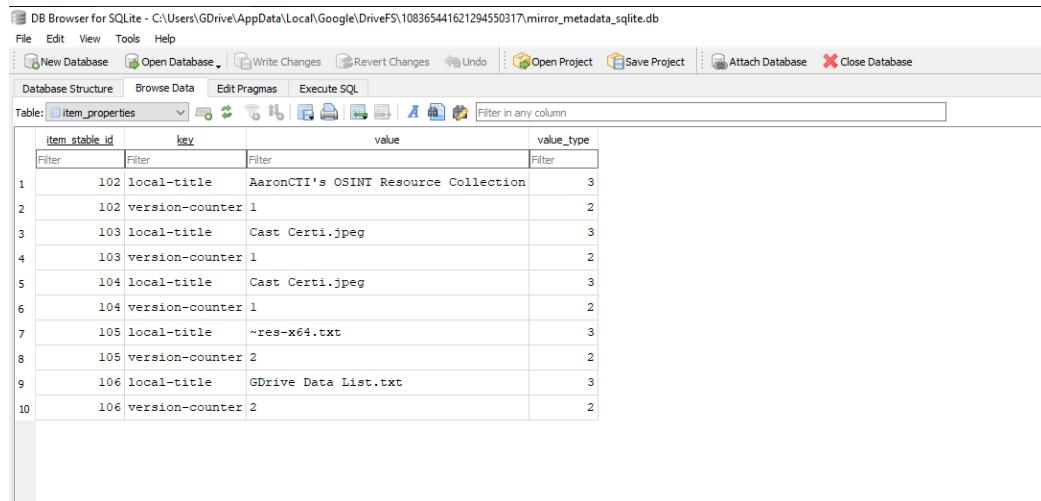
metadata_sqlite_db	11/11/2025 1:58 PM	File	472 KB
metadata_sqlite_db_local_counter_mmap	11/7/2025 4:25 PM	File	1 KB
metadata_sqlite_db-shm	11/11/2025 1:58 PM	File	32 KB
metadata_sqlite_db-vacuum_sentinel.bin	11/7/2025 4:26 PM	BIN File	1 KB
metadata_sqlite_db-wal	11/11/2025 1:58 PM	File	21 KB
metadata_update_db	11/7/2025 4:26 PM	File	28 KB
metadata_update_db-shm	11/11/2025 1:58 PM	File	32 KB
metadata_update_db-wal	11/11/2025 1:58 PM	File	0 KB
metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	24 KB
metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
mirror_cello_metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File	8 KB
mirror_cello_metrics_store_sqlite.db-shm	11/11/2025 1:58 PM	DB-SHM File	32 KB
mirror_cello_metrics_store_sqlite.db-wal	11/11/2025 1:58 PM	DB-WAL File	0 KB
mirror_metadata_sqlite	11/11/2025 1:58 PM	Data Base File	156 KB

Figure 114 : List of DB files created by Drive

Into the updated drive setup the work for the forensics is made easy before that we can check the two file like sync.DB and config.DB but in the but we can check only the mirror_metadata_sqlite.db in this we can have all types details even if the file is permanently deleted from the drive storage that's why also we can see the all file meta data only

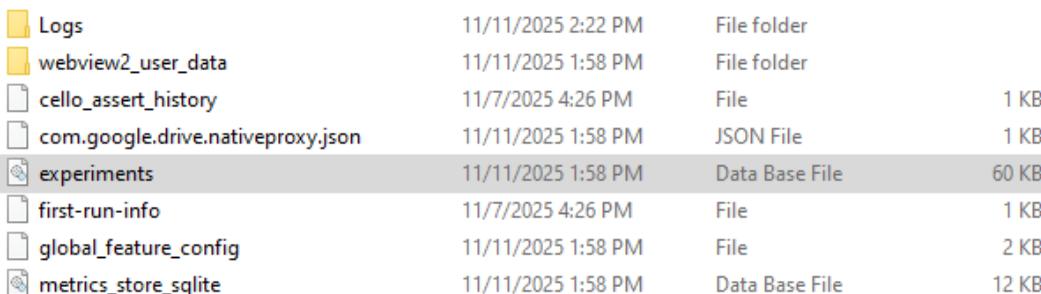
META DATA ARE FOUND DETAILS LIKE:

FILE ID, IS THE FOLDER OR NOT, File type modify date, views date, file size, file title.



item_stable_id	key	value	value_type
1	102 local-title	AaronCTI's OSINT Resource Collection	3
2	102 version-counter	1	2
3	103 local-title	Cast Certi.jpeg	3
4	103 version-counter	1	2
5	104 local-title	Cast Certi.jpeg	3
6	104 version-counter	1	2
7	105 local-title	~res-x64.txt	3
8	105 version-counter	2	2
9	106 local-title	GDrive Data List.txt	3
10	106 version-counter	2	2

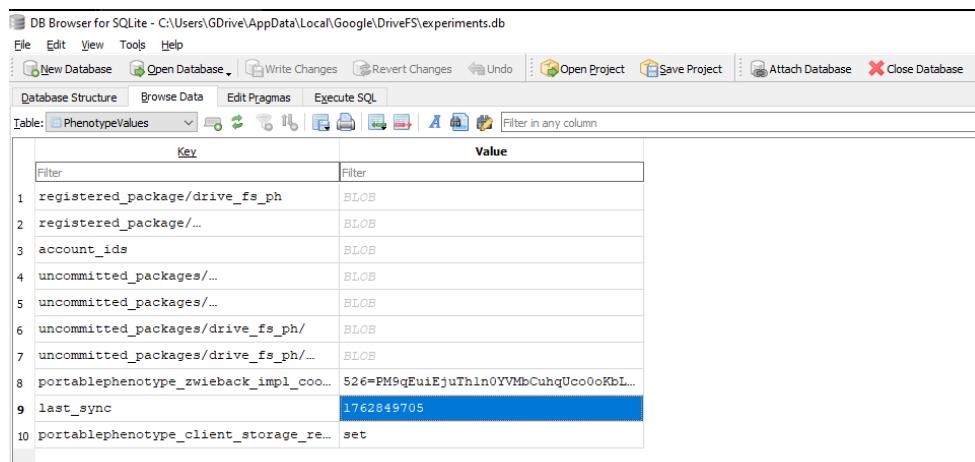
Figure 115 : Sync Data entry DB file



Logs	11/11/2025 2:22 PM	File folder
webview2_user_data	11/11/2025 1:58 PM	File folder
cello_assert_history	11/7/2025 4:26 PM	File
com.google.drive.nativeproxy.json	11/11/2025 1:58 PM	JSON File
experiments	11/11/2025 1:58 PM	Data Base File
first-run-info	11/7/2025 4:26 PM	File
global_feature_config	11/11/2025 1:58 PM	File
metrics_store_sqlite	11/11/2025 1:58 PM	Data Base File

Figure 116 : Data Entry Details with Epoch Time

In the experiment. DB sync data is always-label but it is in epoch time we can converted that time by any online epoch time converter.



Key	Value
1 registered_package/drive_fs_ph	BLOB
2 registered_package/...	BLOB
3 account_ids	BLOB
4 uncommitted_packages/...	BLOB
5 uncommitted_packages/...	BLOB
6 uncommitted_packages/drive_fs_ph/	BLOB
7 uncommitted_packages/drive_fs_ph/...	BLOB
8 portablephenotype_zwieback_coo...	526=FM9qEuiEjuThln0YVMbCuhqUcoOoKbL...
9 last_sync	1762849705
10 portablephenotype_client_storage_re...	set

Figure 117 : Sync DB entry

Convert epoch to human-readable date and vice versa

1762849705 **Timestamp to Human date** [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Tuesday, November 11, 2025 8:28:25 AM

Your time zone : Tuesday, November 11, 2025 1:58:25 PM GMT+05:30

Relative : An hour ago

Figure 118 : File Sync Epoch Time

15.3 RAM dump

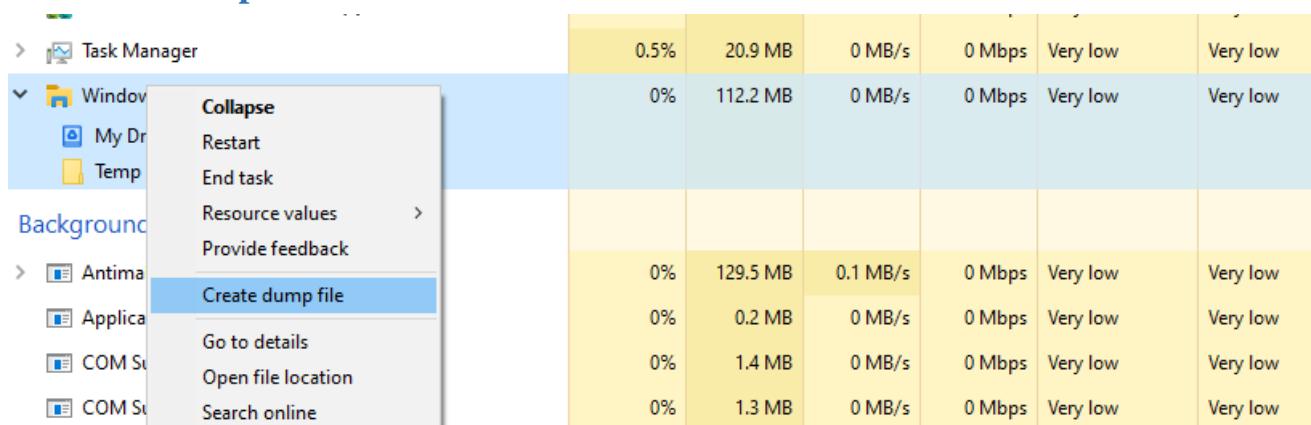


Figure 119 : Ram Dump through Task Manager

We can create a ram dump by FTK imager tools also and from task manager create dump also help for create ram dump.

C : Local Disk (C:) > Users > GDrive > AppData > Local > Temp >				
Name	Date modified	Type	Size	
GoogleDFSSetup_25110/105439_5/68	11/11/2025 4:24 PM	Text Document	191 KB	
explorer	11/11/2025 3:11 PM	DMP File	580,672 KB	
drive_fs_trace	11/11/2025 2:22 PM	File	3 KB	
DO55FF.tmp	11/6/2025 10:35 AM	TMP File	0 KB	

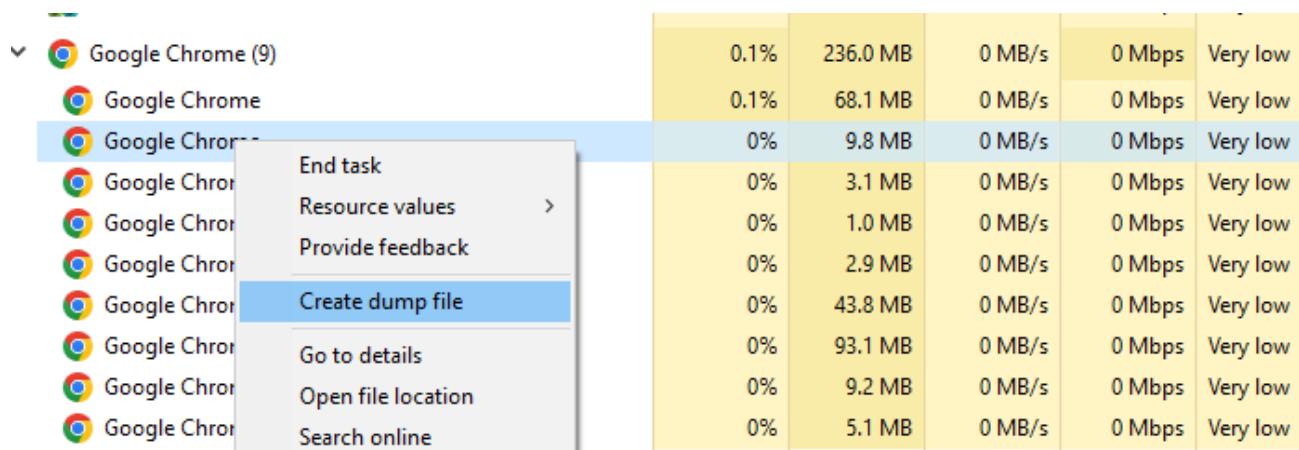
Figure 120 : Ram Dump Files

At the sync time the file was upload to drive at time in ram dump we can see the file name and its destination.

09b0b950	00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 à
09b0b960	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09b0b970	00 00 00 00 00 69 34 be 5c 65 3e 03 88 47 3a 5ci4%\e>.^G:\
09b0b980	4d 79 20 44 72 69 76 65 5c 47 44 72 69 76 65 20	My Drive\GDrive
09b0b990	44 61 74 61 20 4c 69 73 74 2e 74 78 74 00 67 04	Data List.txt.g.
09b0b9a0	18 f9 7f 00 00 6c 34 bd 5c 6c 3f 03 94 01 00 00	.ù...14%\?..."
09b0b9b0	00 00 00 00 00 fo 79 09 10 00 00 00 00 00 00 00öy.....

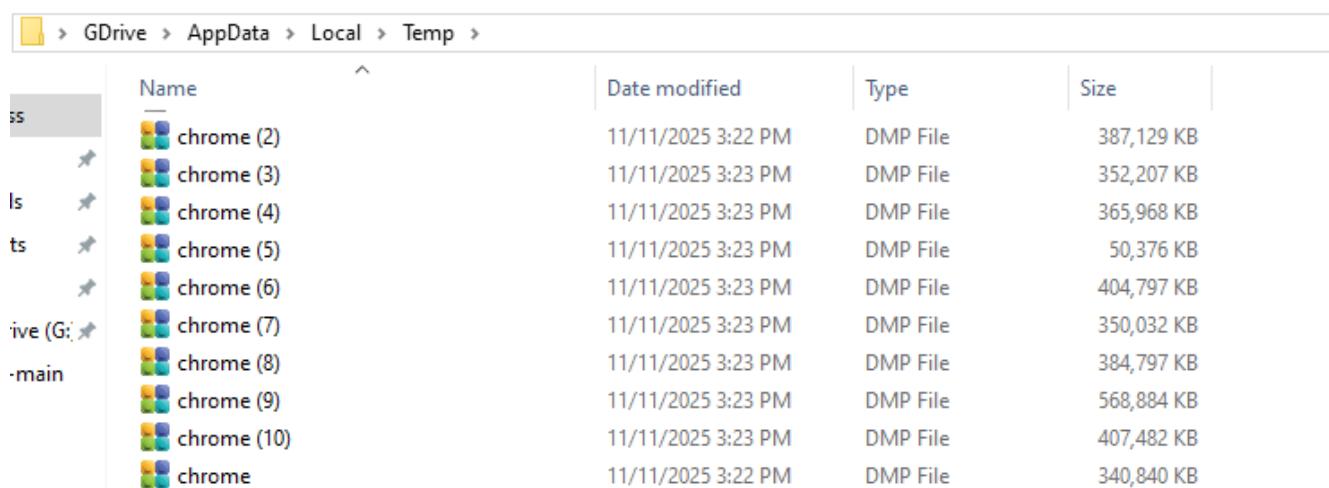
Figure 121 : File Location Reveal at Sync Time

15.4 Browser side forensic



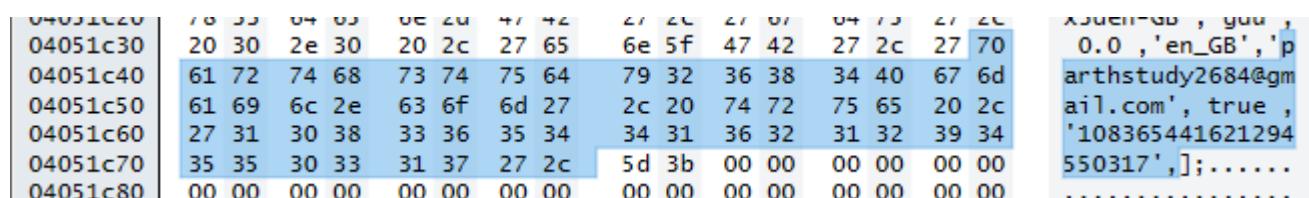
		0.1%	236.0 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome (9)	0.1%	68.1 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	9.8 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	3.1 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	1.0 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	2.9 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	43.8 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	93.1 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	9.2 MB	0 MB/s	0 Mbps	Very low
✓	Google Chrome	0%	5.1 MB	0 MB/s	0 Mbps	Very low

Figure 122 : Dump File Created



	Name	Date modified	Type	Size
ss	chrome (2)	11/11/2025 3:22 PM	DMP File	387,129 KB
ls	chrome (3)	11/11/2025 3:23 PM	DMP File	352,207 KB
ts	chrome (4)	11/11/2025 3:23 PM	DMP File	365,968 KB
ive (G; ↳	chrome (5)	11/11/2025 3:23 PM	DMP File	50,376 KB
-main	chrome (6)	11/11/2025 3:23 PM	DMP File	404,797 KB
	chrome (7)	11/11/2025 3:23 PM	DMP File	350,032 KB
	chrome (8)	11/11/2025 3:23 PM	DMP File	384,797 KB
	chrome (9)	11/11/2025 3:23 PM	DMP File	568,884 KB
	chrome (10)	11/11/2025 3:23 PM	DMP File	407,482 KB
	chrome	11/11/2025 3:22 PM	DMP File	340,840 KB

Figure 123 : Dump File Stored in Temp Folder



04051c30	20 30 2e 30	20 2c 27 65	6e 5f 47 42	27 2c 27 70	0.0 , 'en_GB' , 'p
04051c40	61 72 74 68	73 74 75 64	79 32 36 38	34 40 67 6d	arthstudy2684@gm
04051c50	61 69 6c 2e	63 6f 6d 27	2c 20 74 72	75 65 20 2c	ail.com' , true ,
04051c60	27 31 30 38	33 36 35 34	34 31 36 32	31 32 39 34	'108365441621294
04051c70	35 35 30 33	31 37 27 2c	5d 3b 00 00	00 00 00 00	550317' ,] ;.....
04051c80	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

Figure 124 : Email Id found in Ram Dump

From the browser we can successfully extracted the email id of the user drive in plain text.

15.5 Disk analysis

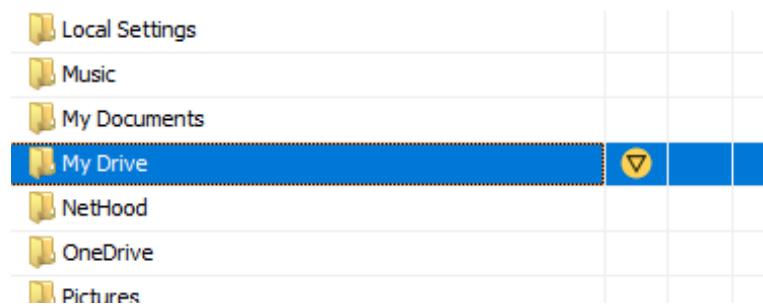


Figure 125 : Find GDrive location

We can find the separated folder in name by my drive in the disk analysis so that we can understand that the Google drive is installed in this user pc.

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Category
GoogleDriveFS.exe				File	Likely Notable		Cloud Storage		Google Stream

Figure 126 : Gdrive installed .exe

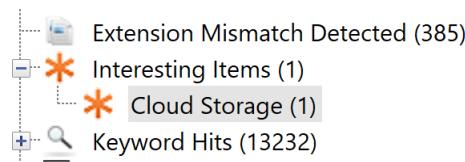


Figure 127 : Autopsy Suggested Cloud installed in this user

WebCacheV01.dat				file:///C:/Users/GDrive/Downloads/Regshot-1.9.0./z
WebCacheV01.dat				file:///C:/Users/GDrive/Desktop/~res-x64.txt
WebCacheV01.dat				file:///C:/Users/GDrive/Desktop/GDrive%20Data%20List.txt
History			1	https://www.instagram.com/stories/jaydipnarigara/

Figure 128 : Browser history

mirror_cello_metrics_store_sqlite.db		0	2025-11-11 13:58:27 IST
mirror_cello_metrics_store_sqlite.db-shm		0	2025-11-11 13:58:33 IST
mirror_cello_metrics_store_sqlite.db-wal		0	2025-11-11 15:44:37 IST
mirror_metadata_sqlite.db		0	2025-11-11 13:58:27 IST
mirror_metadata_sqlite.db-shm		0	2025-11-11 13:58:33 IST
mirror_metadata_sqlite.db-vacuum_sentinel.bin		0	2025-11-07 16:26:07 IST

Figure 129 : Sync DB

108365441621294550317.lnk		C:\Users\GDrive\
Downloads.lnk		C:\Users\GDrive\
DriveFS.lnk		C:\Users\GDrive\
GDrive Data List.lnk		C:\Users\GDrive\
hindsight-main (2).lnk		C:\Users\GDrive\
hindsight-main.lnk		C:\Users\GDrive\
hindsight.lnk		C:\Users\GDrive\
hindsight_gui.lnk		C:\Users\GDrive\
Regshot-1.9.0.7z.lnk		C:\Users\GDrive\
requirements.lnk		C:\Users\GDrive\
setup.lnk		C:\Users\GDrive\

Figure 130 : uploaded successfully document are in lnk

Table PhenotypeValues		6 entries	Page 1 of 1	← →
Key	Value			
account_ids	BLOB Data not shown			
uncommitted_packages/drive_fs_ph/	BLOB Data not shown			
portablephenotype_zwieback_impl_cookie_key	BLOB Data not shown			
last_sync	BLOB Data not shown			
registered_package/drive_fs_ph	BLOB Data not shown			
portablephenotype_client_storage_reset_version_key_2	BLOB Data not shown			

Figure 131 : GDrive DB we can't find the Last sync

Logs			2025-11-11 13:22:10 IST	2025-11-11
webview2_user_data			2025-11-11 13:58:30 IST	2025-11-11
cello_assert_history	0		2025-11-07 16:26:04 IST	2025-11-07
com.google.drive.nativeproxy.json	0		2025-11-11 13:58:31 IST	2025-11-11
experiments.db	0		2025-11-11 13:58:31 IST	2025-11-11
first-run-info	0		2025-11-07 16:26:07 IST	2025-11-07
global_feature_config	0		2025-11-11 13:58:27 IST	2025-11-11
metrics_store_sqlite.db	0		2025-11-11 13:58:30 IST	2025-11-11

Figure 132 : Experiment. DB

metrics_store_sqlite.db-shm	0	2025-11-11 13:58:30 IST	2
metrics_store_sqlite.db-wal	0	2025-11-11 15:12:06 IST	2
pid.txt	0	2025-11-11 13:58:31 IST	2
root_preference_sqlite.db	0	2025-11-11 13:58:28 IST	2
root_preference_sqlite.db-shm	0	2025-11-11 13:58:30 IST	2
root_preference_sqlite.db-wal	0	2025-11-11 13:59:19 IST	2

Figure 133 : Root-Preference.DB

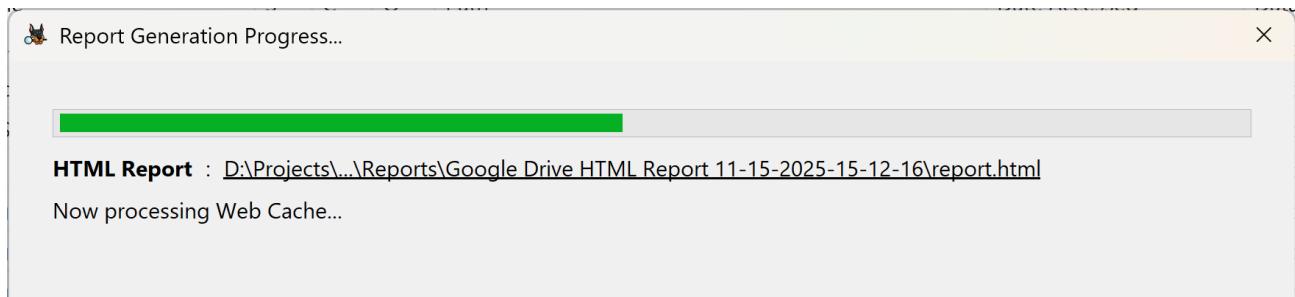


Figure 134 : Google Drive report created successfully

url	2025-11-15 08:56:05.526	https://accounts.google.com/v3/signin/challenge/pwd?TL=ANzgctSKE7-vWJtWelcome	identifier parthstudy2684@gmail.com
autofill	2025-11-15 08:56:06.000		
site setting (engaged)	2025-11-15 08:56:09.288	https://accounts.google.com:443,*	lastEngagementTime in Preference ('last_modified': '13407699369288495', 'site_engagement' in Preference ('last_modified': '13407699369288495'))
site setting (modified)	2025-11-15 08:56:09.288	https://accounts.google.com:443,*	Status: Live last_loaded: 1763225775
site setting (character)	2025-11-15 08:56:15.000	accounts.google.com	fedcm_idp_signin in Preference ('last_modified': '13407699376081717', 'client_hints' in Preferences.profil ('last_modified': '13407699376621692', 'client_hints' in Preferences.profil ('last_modified': '134076993778101365'))
site setting (modified)	2025-11-15 08:56:16.081	https://accounts.google.com:443,*	media_engagement in Preference ('expiration': '13415475377817500', 'last_storageAce - Cookies, Local Storage and Session Storage Manager')
site setting (modified)	2025-11-15 08:56:16.621	https://accounts.youtube.com:443,*	client_hints in Preferences.profil ('last_modified': '13407699404254083', 'client_hints' in Preferences.profil ('last_modified': '13407699405643058'))
site setting (modified)	2025-11-15 08:56:17.401	https://accounts.google.co.in:443,*	
site setting (modified)	2025-11-15 08:56:17.817	https://accounts.google.com:443,*	
url	2025-11-15 08:56:25.945	chrome-extension://cpbgcbmddckpmhfdckolekkhjjmple/src/options/opticStorageAce - Cookies, Local Storage and Session Storage Manager	
site setting (modified)	2025-11-15 08:56:44.254	https://accounts.google.com:443,*	
site setting (modified)	2025-11-15 08:56:45.643	https://drive.google.com:443,*	

Figure 135 : finding a history with auto fill data

local storage	https://drive.google.com	pushNotifications::promoDate::0434984250!1763312215146
local storage	https://drive.google.com	ui:previousBuild drive.web-frontend_20251110.09_p1
local storage	https://drive.google.com	_sak
local storage	https://drive.google.com	pse/591286274:[[[42,1],"043498425050115!Ch9bWzQyLDFdLCIwNDM0OTg0MjUwNTAxMTU1NjIzNyJdEi8KEggBwgYIAA
session storage	https://drive.google.com/	ui:tabFirstStartTimeMsec 1763225811795
session storage	https://drive.google.com/	gapi.sessionStorageTest

Figure 136 : Local and session storage

Account Information	
access_point	66
account_id	108365441621294550317
email	parthstudy2684@gmail.com
full_name	Parth Gondaliya
gaia	108365441621294550317
given_name	Parth
hd	NO_HOSTED_DOMAIN
is_supervised_child	0
is_under_advanced_protection	FALSE
last_downloaded_image_url_with_size	https://lh3.googleusercontent.com/a/ACg8ocJMACBJ-iZnYibf0xLp3jbil1vQKOrZjdTMqlsKcnCpbcpMw=s256-c-n
locale	en
picture_url	https://lh3.googleusercontent.com/a/ACg8ocJMACBJ-iZnYibf0xLp3jbil1vQKOrZjdTMqlsKcnCpbcpMw=s96-c
Local file paths	
Autofill	
enabled	<not present>
Clearing Chrome Data	
clearIsoDataEnabled	<not present>
Per Host Zoom Levels	
Sync Settings	
gaia_id	108365441621294550317
hasSetupCompleted	TRUE

These settings persist even when the history is cleared, and may be useful in some cases.

Figure 137 : email id used to search and profile name

Findings

	Ram Dump			Disk Analysis			Networking
	Email ID	Password	Internal Store password	DB	Sync Plain files	Browsing history	Secured network TLSV2
Pcloud	✓	✗	✓	✓	✓	✓	✓
Mega	✓	✗	-	✓	✓	✓	✓
GDrive	✓	✗	-	✓	✓	✓	✓
OneDrive	✓	✗	✗	✓	✗	✓	✓

Challenges

Cloud environments raise several challenges for forensic examiners. Various research works have proved that traditional investigation approaches are often ineffective or even impossible to apply when working with state-of-the-art cloud services. Among the main challenges, there are geographical, legal, and privacy-related issues.

Cloud investigations are specifically complicated, as they involve thousands of virtual machines, multiple interconnected servers, and large numbers of cloud users—yet only one of these users may be relevant to the case. Collecting evidence from shared infrastructure risks disrupting services for other unrelated users, which is a major concern.

Furthermore, cloud systems operate at the back end, mostly invisible to users. Identity management is often reduced to a level of username and password, which can easily be intercepted or abused due to the open and distributed nature of the cloud. It is tough to ensure the authenticity of user activity since there is no physical control or interaction.

There is also a considerable shortage of dependable tools that are especially purposed for cloud forensics. The cloud ecosystem is very diverse, ranging from different platforms to diverse architectures, leading to a lack of standardization. This fragmentation makes it difficult to develop effective forensic tools capable of extracting data across multiple cloud environments.

Conclusions

Cloud technology growth and increased capability are rapidly changing the face of digital forensics. The aim of this project was to investigate cloud storage platforms and analyze how files, whether existing or deleted, can be analyzed and recovered. Our findings show that a number of artifacts remain even after files are deleted or after cloud storage applications are uninstalled. The number and type of artifacts vary depending on such actions as file creation, deletion, transfers, and movements within the application.

Different tools for virtualization security play an important role. Some provide general security functions like antivirus or backup, while others focus on the security of cloud environments or virtual machines. Since each type of tool serves a different purpose, organizations often deploy multiple solutions together-especially for applications handling sensitive or business-critical data.

Based on the forensic analyses performed in this work, some of the key observations include:

- Valuable information can be recovered by analyzing artifacts left behind by cloud storage clients.
- Google Drive uses **SQLite databases** to store file-related information.
- Google Drive should ideally implement encryption for its database files.
- The **mirror.log** file in Google Drive contains useful details about deleted files.
- RAM analysis can reveal configuration details and, in some cases, user identifiers or passwords.
- Traditional Windows artifacts can provide additional information relevant to the investigation.
- Although recovering evidence of deleted files is challenging, careful log analysis can often retrieve it.
- The **OneDrive SyncDiagnostics.log** file is helpful for examining recent synchronization activities.
- Traditional Windows artifacts such as browser history, thumbnails, and *pagefile.sys* also contain relevant evidence.
- Password recovery for OneDrive, MEGA, or pCloud Crypto is extremely difficult due to strong encryption.

References

<https://www.geeksforgeeks.org/cloud-computing/history-of-cloud-computing/>

<https://www.cogentinfo.com/resources/the-evolution-of-cloud-computing-trends-and-emerging-technologies-shaping-2025>

<https://www.acte.in/introduction-to-cloud-computing>

[Cloud computing - Wikipedia](#)

[Cloud Computing Architecture \(tutorialspoint.com\)](#)

[Personal Cloud Storage – Microsoft OneDrive](#)

<http://www.123seminarsonly.com/CS/Cloud-Storage.html>

https://www.zte.com.cn/global/about/magazine/zte-communications/2010/4/en_140/197075.html?utm_source=chatgpt.com

<https://www.securestorageservices.co.uk/article/11/pros-and-cons-of-cloud-storage>

<https://www.geeksforgeeks.org/cloud-computing/10-advantages-and-disadvantages-of-cloud-storage/>

Literature review:

<https://www.securityblue.team/blog/posts/cloud-surfing-google-drive-forensics>

Cloud Surfing: Riding the Waves of Google Drive Forensics (2024)

<https://orbit.dtu.dk/en/publications/cloud-storage-client-forensic-analysis-of-mega-cloud/>

Cloud Storage Client Forensic: Analysis of MEGA Cloud (2024)

<https://www.semanticscholar.org/paper/Cloud-Forensic-Analysis-on-pCloud:-From-Volatile-AhmadHamid/70ac9c8b4e22fecc50e52ce77bd174e4636fe2c4>

Cloud Forensic Analysis on pCloud: From Volatile Memory Perspectives (2022-2023)

<https://cyberengage.org/onedrive-forensics/>

OneDrive Forensics: Investigating Cloud Storage on Windows Systems (2025)