“CLOUD STORAGE FORENICS”

A Report submitted

In partial fulfilment for the Degree of

MASTER OF SCIENCE

IN

DIGITAL FORENSICS & INFORMATION SECURITY

Submitted By

PRAJAPATI HIMIL HARSHADKUMAR

(012200300003011)

Under the Supervision of

DR. NILAY MISTRY

(Associate Professor)

Submitted to

SCHOOL OF CYBER SECURITY & DIGITAL FORENSICS,

NATIONAL FORENSIC SCIENCES UNIVERSITY

GANDHINAGAR – 382009, GUJARAT, INDIA.

JULY, 2023

DECLARATION

I **Prajapati Himil Harshadkumar** having Enrollment Number **"012200300003011"** hereby declare that The work reported in the M.Sc. Digital Forensic & Information Security entitled "Cloud Forensics" submitted at Institute of Forensic Science, National Forensic Sciences University is an authentic record of my work carried out under the supervision of Dr. Nilay Mister. I have not submitted this work elsewhere for any other degree. I am fully responsible for the contents of my Dissertation.

Date: 7-1-2023
Place: Institute of Forensic Sciences
National Forensic Sciences University,
Gandhinagar

Signature of Student

CERTIFICATE

This is to certify that the work contained in the dissertation entitled **"Cloud Storage Forensics"**, submitted by **Prajapati Himil Harshadkumar (Enroll. No.: 012200300003011)** in partial fulfilment of the requirement for the award of the degree of **M.Sc. Digital Forensics & Information Security** to the **National Forensic Sciences University**, **Gandhinagar, Gujarat** is a record of bonafide work carried out by him under my direct supervision and guidance.

Date: 7-1-2023
Place: Institute of Forensic Sciences

National Forensic Sciences University,

Gandhinagar

Signature & Date

Supervisor(s)

ACKNOWLEDGEMENTS

It Gives us immense pleasure in expressing thank and profound gratitude to Dr. S O Junare , honourable director, Institute of Forensic Sciences, National Forensic Sciences University, Gandhinagar for their kind support and providing basic infrastructure and healthy research environment.

I am thanking to Dr. Nilay Mistry who provided me such motivation and Guidelines and I am also thanking to Dr. Digvijaysinh Rathod & Mr Dharmesh Dave from the National Forensic Sciences University to helping out during the project.

I would also thank the institution, all classmates of Digital Forensics, Institute of Forensic Sciences, National Forensic Sciences University, Gandhinagar for their special attention and suggestions towards the project work.

With Sincere Regards,

Prajapati Himil Harshadkumar

Digital forensics and information security

ABSTRACT

Cloud storage and Cloud servers, it has become easier than ever to backup all our important computer files online. We are now given the flexibility of accessing all our files from anywhere in the world, with the benefit of knowing that all our important pictures, videos, music, files, documents, as well as other programs and data are securely stored and available to us 24 hours a day 7 days a week.

Cloud forensics is the practice of collecting and analysing digital evidence from cloud computing systems in order to investigate and solve criminal cases or security incidents. As more organizations are moving their data and applications to the cloud, cloud forensics has become increasingly important in the field of digital forensics.

The main challenge in cloud forensics is the fact that data is stored in shared infrastructure and is spread across multiple geographic locations, making it difficult to access and preserve evidence. Therefore, cloud forensics requires specialized techniques and tools to acquire and analyse evidence from cloud computing environments.

Some of the key challenges in cloud forensics include identifying relevant data sources, preserving evidence integrity, and maintaining chain of custody. Furthermore, cloud computing environments are subject to constant change, making it difficult to maintain an accurate and up-to-date record of the system state.

This technology can be misused and it can lead to violation of laws governing the cyber world. One of the approaches to this scenario is to perform digital forensics when cybercrime has occurred which is the focus of this project.

This Project Presents the cloud forensic for process and a so more briefly describe about the cloud forensic investigation like stand alone and web-based cloud forensic, and find the evidence from disk image analysis. Digital forensics is based on scientifically proven methods to collect and analyse digital information.

LIST OF FIGURES

TABLE OF CONTENTS

1. Introduction

1.1 Purpose

The fast advancement and increase in quality of cloud technology is definitely pushing digital forensic to entire new level. The main goal of the project was to perform investigation in the cloud storage. How we can investigate and try to retrieve the files, which have been present, have been deleted .we conclude that various antiques are deserted after the erasure cloud storage the quantity of antiques that were influenced upon creation, cancellation, transferring and moving inside the application shifted.

1.2 Introduction to cloud computing

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

Cloud Computing referred as the accessing and storing of data and provide services related to computing over the internet. It simply referred as it 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.

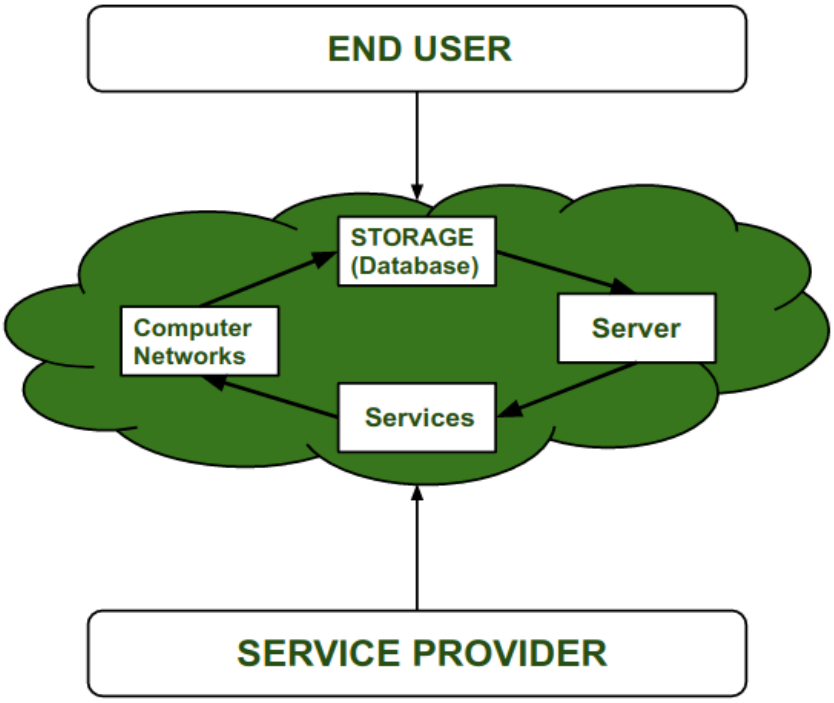


Figure 1 flow of cloud

1.3 Cloud computing service provider's

Cloud computing is in huge demand so, big organization providing the service like Amazon AWS, Microsoft Azure, Google Cloud, Alibaba cloud etc. are some Cloud Computing service Provider.

1.4 Term cloud computing

The term "cloud computing" was coined to describe the concept of delivering computing services over 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 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 Computing was come into existence, client Server Architecture was used where all the data and control of client resides in Server side. If a single user want to access some data, firstly user need to connect to the server and after that user will get appropriate access. But it has many disadvantages. So, After Client Server computing, Distributed Computing was come into existence, in this type of computing all computers are networked together with the help of this, user can share their resources when needed. It also has certain limitations. So in order to remove limitations faced in distributed system, cloud computing was emerged.

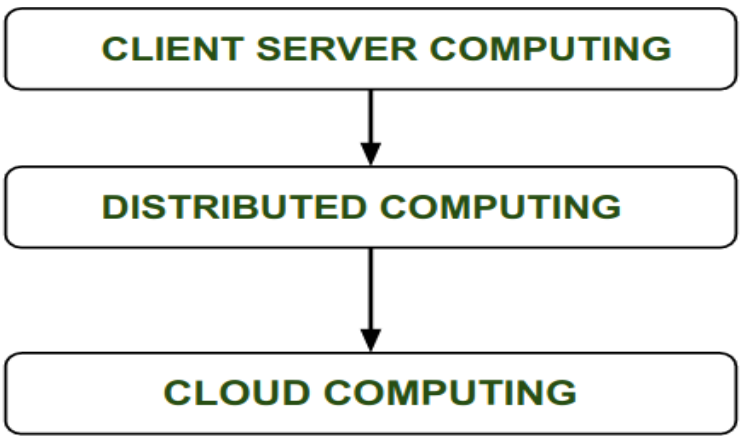


Figure 2flow of work

During 1961, John MacCharty delivered his speech at MIT that "Computing Can be sold as a Utility, like Water and Electricity." According to John MacCharty it was a brilliant idea. But people at that time don't want to adopt this technology. They thought the technology they are using efficient enough for them. So, this concept of computing was not appreciated much so and very less will research on it. But as the time fleet the technology caught the idea after few years this idea is implemented. So, this is implemented by Salesforce.com in 1999.

This company started delivering an enterprise application over the internet and this way the boom of "**Cloud Computing**" was started

- In 2002, Amazon started Amazon Web Services (AWS), Amazon will provide storage, computation over the internet.
- In 2006 Amazon will launch Elastic Compute Cloud Commercial Service which is open for everybody to use.
- 2006: Google launches Google Docs End users were directly able to use cloud computing for document sharing purposes.
- 2007: Dropbox MIT student created this file hosting service that offers file storage and synchronization

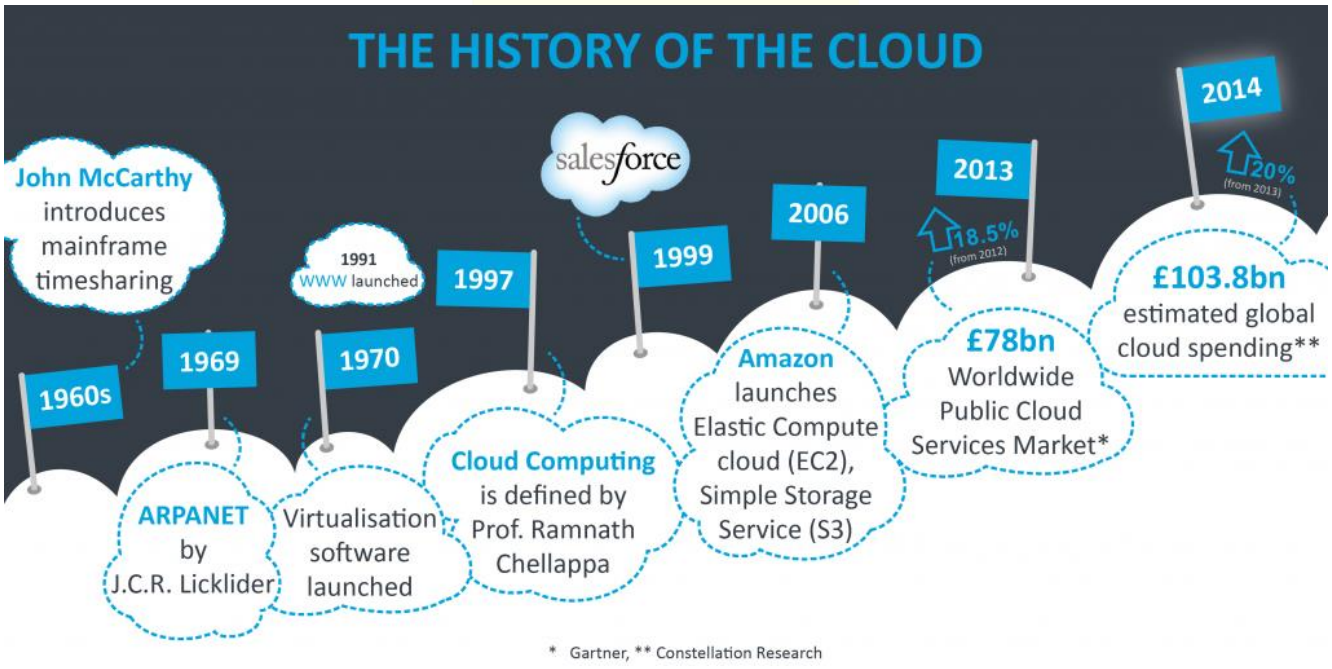


Figure 3 Time line of cloud History

- In early 2008, NASAs Open Nebula, enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid clouds

- After that in 2009, Google Play also started providing Cloud Computing Enterprise Application as other companies will see the emergence of cloud computing they also started providing their cloud services.

- Another big milestone came in 2009, as Web 2.0 hit its stride, and Google and others started to offer browser-based enterprise applications, though services such as Google Apps.

- In 2009, Microsoft launch Microsoft Azure and after that other companies like Alibaba, IBM, Oracle, and HP also introduces their Cloud Services. In today the Cloud Computing become very popular and important skill.

- From the "March 2013" the **docker container** and from "9th September 2014" the **Kubernetes** was released originally developed by Google, who needed a new way to run billions of containers a week at scale. Google notes that Kubernetes' "main design goal is to make it easy to deploy and manage complex distributed systems.

- Kubernetes bundles a set of containers into a group that it manages on the same machine to reduce network overhead and increase resource usage efficiency. An example of a container set is an app server, redis cache, and sql database. Docker containers are one process per container.

- In 2022, the web will be transformed by a third version, commonly known as "Web 3.0."

2. Background study/ Literature review

Literature review helps us a great extent to acquire knowledge about a research area. First phase of the research started with literature review and Cloud Storage forensic by Mattia Epifani Client Application on the Windows Platform presented SANS European Digital Forensic Summit.

2.1 Digital Forensics Investigation on cloud storage services by (HyunjiChung, JungheumPark, SangjinLee, CheulhoonKang) [1]

The demand for cloud computing is increasing because of the popularity of digital devices and the wide use of the Internet. Among cloud computing services, most consumers use cloud storage services that provide mass storage. This is because these services give them various additional functions as well as storage. It is easy to access cloud storage services using smartphones. With increasing utilization, it is possible for malicious users to abuse cloud storage services. Therefore, a study on digital forensic investigation of cloud storage services is necessary.

2.2 Cloud Storage Forensics by (Darren Quick, Ben Martini, Raymond Choo) [2]

Cloud Storage Forensics presents the first evidence-based cloud forensic framework. By determining the data remnants on client devices, you gain a better understanding of the types of terrestrial artifacts that are likely to remain at the Identification stage of an investigation. Once it is determined that a cloud storage service account has potential evidence of relevance to an investigation, you can communicate this to legal liaison points within service providers to enable them to respond and secure evidence in a timely manner.

Context of these paper is to conduct a forensic analysis of cloud client storage on a Windows 7 virtual machine. To find all the possible traces left on the system that uses the cloud storage application and try to find the traces even after the application is deleted from the system.

2.3 Cloud Storage Client Forensic: Analysis of MEGA Cloud by (Vikas Sihag, Himanshu Mishra's, Gaurav Choudhary, Nicola Dragoni) [3]

This investigative study focused on analyzing forensic artifacts related to the usage of the MEGA cloud storage service across different platforms (Google Chrome browser, Windows application, and Android application). The study successfully recovered various artifacts such as account name, email address, network information, username, and MD5 hash verification of original and downloaded files. Changes in metadata timestamps were observed, and client credentials were recovered. Although the user password could not be located in memory dump or storage, offline strategies were suggested. A forensic investigation on the client side involved recovering and analyzing artifacts from the client machine.

2.4 Cloud forensics: Technical challenges, solutions and comparative analysis by (Ameer Pichan, Mihai Lazarescu, Sie Teng Soh) [4]

This paper addresses the concerns surrounding the security, privacy, and potential misuse of cloud computing services. With the increasing adoption of cloud technology, there is a need to understand and mitigate the risks associated with cybercrimes facilitated by cloud platforms. The paper presents a systematic analysis of the challenges faced in cloud forensics and proposes solutions for each phase of the forensic process. It highlights the maturity of existing solutions while identifying opportunities for further research and development. Additionally, a summary of forensics-as-a-service models is provided as a potential approach to address forensic difficulties in cloud environments.

2.5 Forensic Analysis of Google Drive on Windows by (Ming Sang Chan) [5]

When we investigate the using of cloud storage, the initial stages include the identification of a cloud service and user account. This may enable investigators to identify the location of data. In this research, we find that an investigator can identify Google Drive account use by undertaking keyword searches and examine test files locations to locate relevant information. The remnants of cloud activity can be found on local machines. It could be valuable for the forensic examiners. We found the remnants in local folders. The username, the cache files, and log activity which helps in recovering the deleted files and data. We identify the locations of data and files to determine user details and cloud storage information relating to use of Google Drive in our research

3. Important components of cloud architecture

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

1. Front ends
2. Back ends

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:

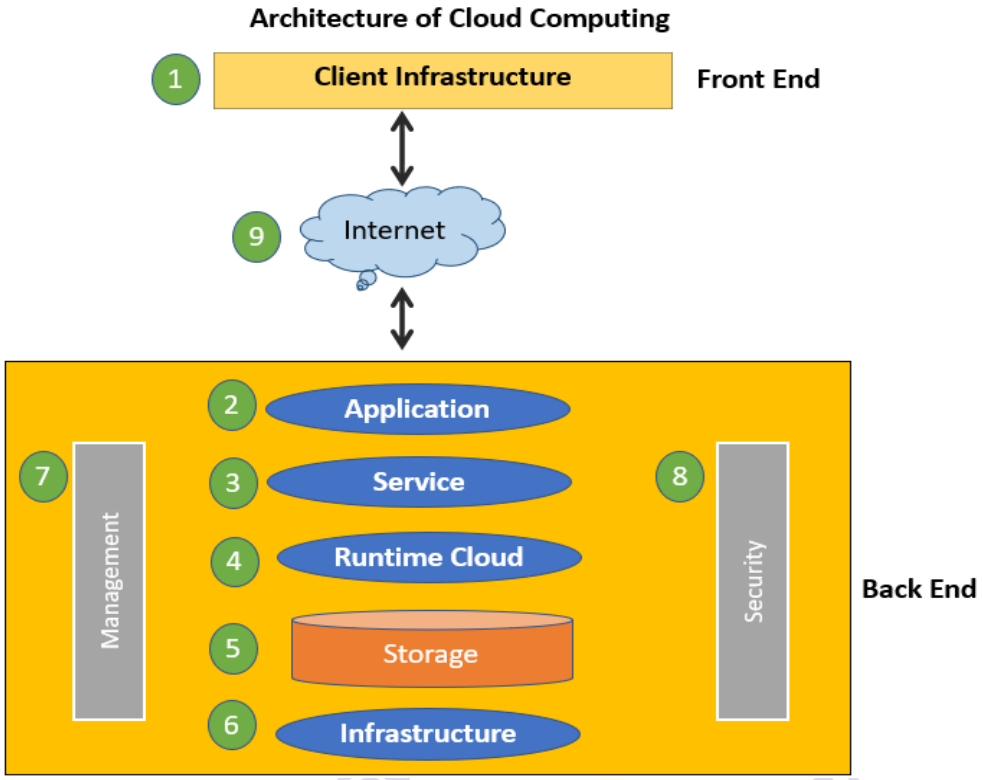


Figure 4 general Cloud Components

The Architecture of Cloud computing contains many different components. It includes Client infrastructure, applications, services, runtime clouds, storage spaces, management, and security. These are all the parts of a Cloud computing architecture.

3.1.1 Front end:

The client uses the front end, which contains a client-side interface and application. Both of these components are important to access the Cloud computing platform. The front end includes web servers (Chrome, Firefox, Opera, etc.), clients, and mobile devices.

3.1.2 Back end:

The backend part helps you manage all the resources needed to provide Cloud computing services. This Cloud architecture part includes a security mechanism, a large amount of data storage, servers, virtual machines, traffic control mechanisms, etc.

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 or hybrid cloud.

3.2.1 Public cloud:

The third-party cloud service provider owns and runs the business of providing cloud computing 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 Efficiency / cost reduction:

Deploying cloud computing technology saves the organization a lot of money on the purchase and period maintenance of hardware. There is a reduction in investment in facilities, hardware utility or constructing a bigger data center as the business grows. You need not keep a Full time IT team to handle the cloud infrastructure as you can the cloud service provider give a team to work with. Using Cloud service passes the cost related to manage downtimes. Since downtime is almost absent in cloud systems, this means more time to concentrate on core business operations.

4.2 Data security:

The security of an organization's data/information is crucial to the survival of the business. The organization cannot afford the cost of Data breaches as a result of cyber-attacks. This is very devastating on the company's revenue, customer retention, and brand-Cloud technologies service providers adopt advanced-level security features and system the makes sure that customers data is secure from attacks They also implement different levels of protection for their platforms and the data they handle such access control, authentication and encryption Many companies take other auxiliary backup security mechanisms just to boost and tighten access to confidential and sensitive data in eh cloud

4.3 Scalability:

The information technology need of every organization is different and they are not on the same level in terms of the business operations; size, technology infrastructure requirements. A big enterprise of over 2000 employees would not have the same technical requirements as a start-up business. Using cloud technologies can be a leverage for both large and small enterprise to scale up or down their information technology resources in parallel to the operations of the business Cloud Computing technologies are perfect for companies with an increase or unstable technology resource requirements.

It provides the flexibility to adjust your cloud technology resource needs as when the need arises without investing in the acquisition of physical the level of flexibility makes businesses that employ the cloud technology competitive advantage.

The ease with scaling the cloud service to meet growing needs reduces the risk associated with running own infrastructure with the organization this is the greatest advantage of adopting cloud technology of solution.

5. Cloud storage architecture

Cloud storage differs from traditional storage in many aspects. In terms of its operations, it is created to deliver many online storage services, whereas conventional storage systems are basically created for high-performance computation and transaction processing. In terms of performance, cloud storage places great importance on data security, reliability, and efficiency. With a larger number of users, a wider service range, and a complex and ever-changing network environment, cloud storage systems face greater technical challenges than traditional systems when delivering high-quality services. In terms of data management, cloud storage systems not only offer access to traditional files such as Portable Operating System Interface for Unix (POSIX), but also support mass data management for providing public service support functions, and maintaining data in the background.

A cloud storage platform can be classified into four layers: data storage layer, data management layer, data service layer, and user access layer. Figure I shows the architecture of a cloud storage platform as proposed by (Zhou Ke ET el 2010)

5.1 Data storage layer:

A cloud storage system offers divers storage sea-vices and all data stored in the system form a massive POOL For efficient storage, this data should be properly organized in the system. Traditional data organization uses a single server and cannot meet the throughput and storage capacity requirement of multiple users in a Wide Area Network

A peer-to-peer architecture-based organization method requires a large number of nodes and complicated coding algorithm to ensure data reliability comparatively using different storage services to arrange data is suitable for online storage services

Data center scattered around can provide the best quality of service for a greater number of users in diverse locations and regions

The interconnection of different types of storage devices that the storage layer can manage huge amounts of data in a consolidated approach and can employ centralized management, status monitoring, and dynamic capacity expansion of storage devices. Cloud Storage systems as mainly service-oriented distributed storage systems.

5.2 Data management layer:

The Data Management layer provides a higher layer with a public Management interface for different services. It has functions such as user management. Security management, Replica management, and strategic management. The layer seamlessly attaches upper layer applications with lower layer storage services.

The layer also promotes cooperation between storage devices, enabling them to provide diverse and enhanced service

5.3 Data service layer:

This layer interacts directly with the user and can easily be manipulated. Depending on user requests, different application user interfaces can be developed to provide service like data storage, space leasing, a public resource, multi-user data sharing or data backup

5.4 User access layer:

The layer makes it possible for authorized users to log into the cloud storage platform from any location through a standard public application interface and access cloud storage

6. Advantages/disadvantage of cloud storage

The main advantage of these services as Goggle 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 is 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 Cloud storage can Save costs:

Based on the scale they operate cloud storage service providers benefit from buying lots of storage which the transfer to their customers as discounts which is a great cost-saving for the customers who engage them. Customers also befit from the need to buy more Gigabytes of physical storage as the business grows.

Cloud Storage services provide RAID (Redundant Array of Inexpensive Disk) service and this goes a long way to reduce the cost of maintenance as management gets to concentrate on business other than the technology solutions functionality. That is handed by the cloud technology service providers

6.1.2 Data replication and redundancy:

As indicated above data redundancy and its replication is a paramour.t feature in cloud storage service. Service providers keep multiple copies of your data in different data center at different locations. This important to prevent attacks, data loss due to security breaches like a cyber-attack, other value-added service rendered by Cloud technology service providers is the option to

6.1.3 Data packaging for cost savings:

Many cloud storage companies offer different data storage packages. The business chooses the package that is suitable for their current needs and bundles up as their needs grow. The decision of a package is taking upon a clear analysis of the business process and the amount of data it generates through the company

6.1.4 Regulatory compliance:

There regulation on data storage and handling in many jurisdictions of the work. Several government agencies set guidelines on how the is handled. Some of these guidelines are due to the industry the organization operates. It may require the business to store their data with the territory of the state. For this reason, Many Cloud storage service providers have data center all over the world. They try best to store your data at a location close to you.

6.1.5 Malware protection:

Protecting one's information again malicious attacks especially malware that have devastating impact on the organization. Cloud storage service providers protect information from such attacks even though they might have attacked the organization's infrastructure on the premise. Due to the authentication and advance security measure implemented it will next to impossible for the data center to be infected with such malware

6.2 Disadvantages of cloud storage

In as much Cloud storage has several advantages, it also has some drawback which includes:

6.2.1 Dependency on internet speed:

It is difficult to access cloud services with a slow internet connection. Reliable and fast internet connectivity needs if organizations need to constantly access a resource in the cloud. Enough bandwidth is required

6.2.2 Dependency on a third party:

Through research and due diligence need to be conducted in selecting the cloud storage service provider. Key among the criteria is Information Security and Best operation standards

6.2.3 High cost for big data:

Companies that generate a lot of data require a large amount of storage space which may also translate into an increase in cost.

6.2.4 Minimal control over data storage framework

Cloud Storage service provider is responsible for the management of the cloud infrastructure and the customer has no or minimal control over it.

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 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 be 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 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 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 user create documents, images, emails and surf the internet. These activities leave traces on the computer which are good source digital evidence. The actual files may not reside on the local machine and such the forensic expert many rely on artifacts Len behind on the system to able to trace user activities

The logs recorded by the cloud service provider can provide audit trails of user acclivities, this information is however kept private and protected by the cloud storage service provider.

8. Problem statement

8.1 Digital forensic in cloud computing:

More and more organisations and individuals are relaying on cloud computing to host their services, applications and data. This proliferation of cloud computing has brought many challenges to forensic investigators as they rarely have physical access to the underlying infrastructure. The amount of data these cloud providers have from their clients is a very desirable objective for criminals. Additionally, cyber-crooks can use cloud computing as a platform to distribute malware, conduct scams and perform other criminal activity. Thus, investigating cloud related crimes is an arduous but essential task in order to bring criminals to justice.

8.2 Developing a cloud forensics strategy:

Organizations face numerous federal and state laws relating to the preservation of information related to taxes, securities and employment regulation. At the same time, they need to maintain compliance with other laws relating to the destruction of information that is no longer needed. Cloud computing also raises new questions about who owns the data and the customer's expectations of privacy. Laws vary on the legal protections regarding data in the cloud from country to country.

8.3 Security and Forensic Issues Concerning Cloud Computing:

With the huge amount of potential data flowing in and out of a cloud, how do you identify individual users of individual services provided by a transient host image, particularly when they make expert efforts to cover their tracks? And what if the owner of the image decides to engage in malicious behaviour, through the host server image, from a third IP address, and then claim someone must have stolen their password or key pair to the image?

Further forensic issues concern the potential effect the cloud services could have on the digital data itself and how the forensic examiner can explain, in a creditable manner, all these real and potential indiscretions to the court. Many forensic examiners recognize that 'there is no fool proof, universal method for extracting evidence in an admissible fashion from cloud-based applications, and in some cases, very little evidence is available to extract.

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
- Repotting

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 device(s) from the scene of the crime and taking then creating a bit-by-bit copy of it, or printing. Whichever way the evidence its 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 arc taken through the investigation process. This recorded 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 is experimental research that involves a practical demonstration of identification, collection preservation analysis and presentation results of the experiment. The experiment is conducted with Cloud Storage Service Google Drive, OneDrive, MegaSyn and Pcloud Service.

There are two activities to conduct analysis on:

- Browser interactions
- Client Application interactions

The experiments include the following activities in the 2-cloud storage service using the Client application and web Browser

File Download

File Upload

File Deletion

File Sharing

Because we may not have access to the data center of Cloud service provider in other to carry out thorough forensics investigation, we rely on evidence of Past Data Possession on the user computer system (Sham Zawoad. ET el 2012)

10.1 Flow of work

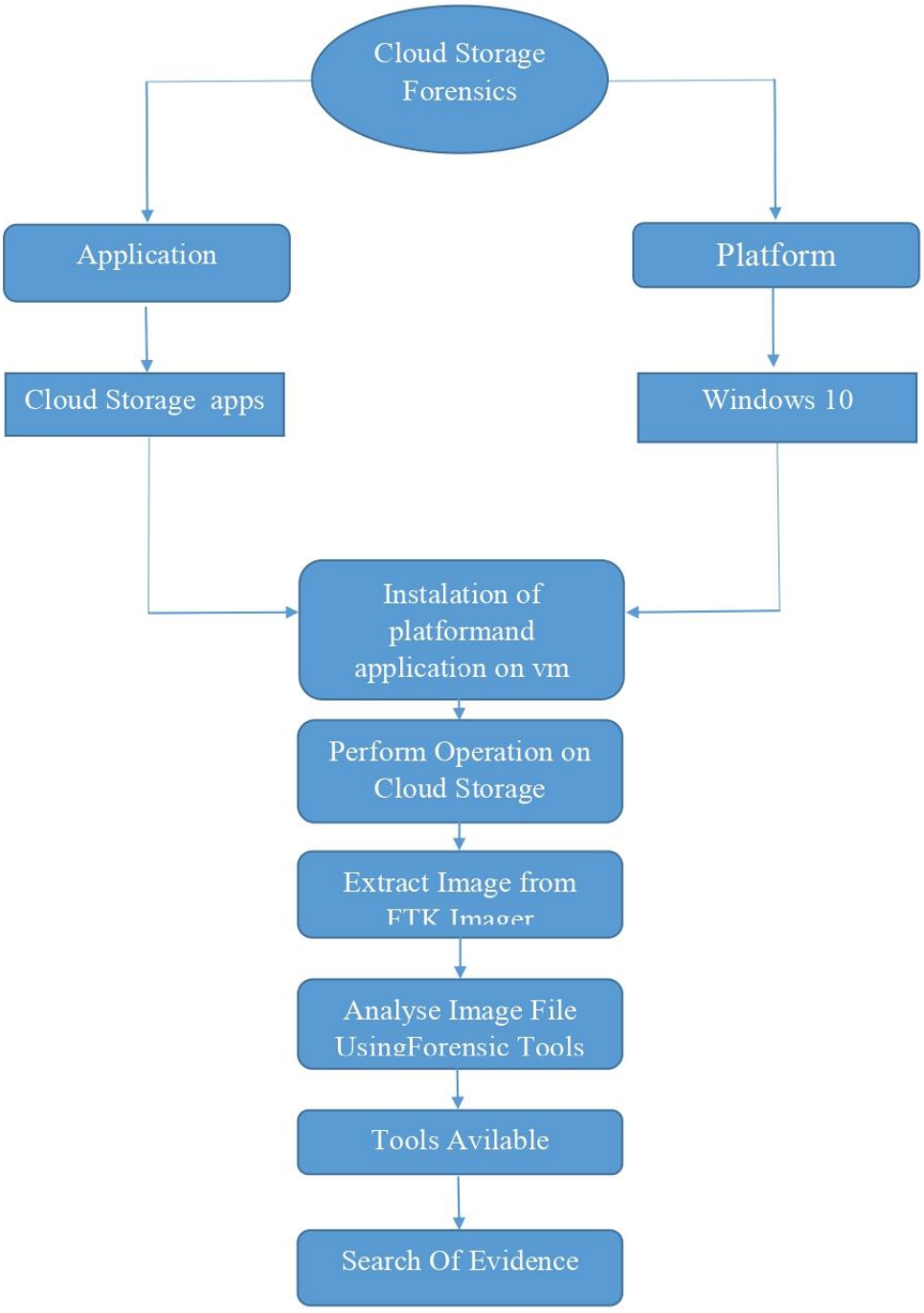


Figure 5 Work Flow

11. Tools

11.1 Autopsy forensic tool

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

11.2 Easy to use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details.

11.3 Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).

Hash Filtering - Flag known bad files and ignore known good.

Keyword Search - Indexed keyword search to find files that mention relevant terms.

Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.

Data Carving - Recover deleted files from unallocated space using PhotoRec

Multimedia - Extract EXIF from pictures and watch videos.

Indicators of Compromise - Scan a computer using STIX.

See the Features page for more details. Developers should refer to the module

Development page for details on building modules.

There is currently an Autopsy Module Writing Contest going on right now before

OSDFCon 2016. Start writing modules for cash prizes.

11.4 Fast

Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the fast results page for more details.

11.5 Cost effective

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

Product Version: Autopsy 4.4.1

Sleuth Kit Version 4.20.0

Platform 64 bit

Company BASIS TECHNOLOGY

11.6 FTK Imager 4.7.1.2

The Forensic Toolkit Imager (FTK Imager) is a commercial forensic Imaging software package distributed by Access Data. The FTK toolkit includes a standalone disk-imaging program called FTK Imager. The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files. In addition to the FTK Imager tool can mount devices (e.g., drives) and recover deleted files.

11.7 Hex editor neo

Free Hex Editor Neo is the fastest 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 profiling network traffic and analysing packets. Such a tool is often referred to as a network analyser, network protocol analyser or sniffer.

11.9 VMWare

VMware is a virtualization and cloud computing software vendor based in Palo Alto, California. Founded in 1998, VMware is now a subsidiary of Dell Technologies. VMware bases its virtualization technologies on its bare-metal hypervisor ESX/ESXi in x86 architecture.

11.10 Hindsight

Hindsight is a free tool for analyzing web artifacts. It started with the browsing history of the Google Chrome web browser and has expanded to support other Chromium-based applications (with more to come!). Hindsight can parse a number of different types of web artifacts, including URLs, download history, cache records, bookmarks, autofill records, saved passwords, preferences, browser extensions, HTTP cookies, and Local Storage records (HTML5 cookies). Once the data is extracted from each file, it is correlated with data from other history files and placed in a timeline.

12. Pcloud storage service

Pcloud is one of the widely accepted cloud storage services that takes pleasure in presenting the very best safety with unlimited add and download speeds. It's been around considering the fact that 2013, having benefited from the successes and failures of the competition. It's far a few of the first cloud storage offerings to offer lifetime plans. Considering the fact that there is no limit to the dimensions of your documents or the download speeds. It has top-notch security with a backup feature. Like other cloud storages e. G. Google force, drop box, and so on, you could lower back up your social media debts (Instagram, Facebook, and Picasa) and your Word press websites. You may also upload your files as "favourites" to get right of entry to them while offline. In this manual, I will show you a way to use cloud and all of its functions.

12.1 File synchronisation

The PCloud app and web interface permits multiple file-sharing options and one could always send folders and files to any location you choose. The additional virtual drive lets you able to expand your computer and all files uploaded to that folder can be accessed to you in any device. Anywhere anyhow.

Open your PCloud drive in your file manager with a quick left-click or right-click on the indicator. Open your crypto folder if you have already subscribed and then add new folders to the Sync. Other options include checking your account status and notifications.

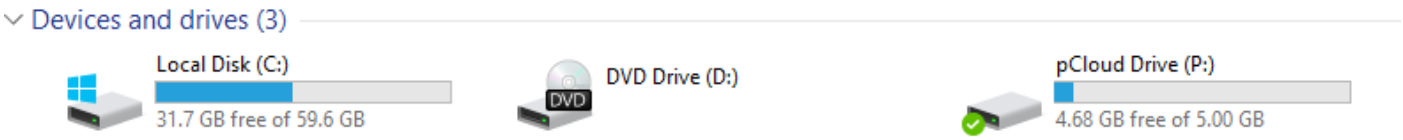


Figure 6 Pcloud Local Drive

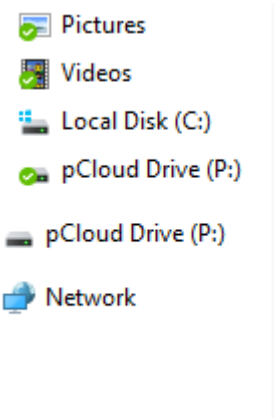


Figure 7 Pcloud listed in the Drive list

12.2 To add a new local folder to the sync:

1. Open the PCloud panel and click "Sync"

2. Click "Add New" and then choose the local folder

3. Navigate to the folder you want to sync

4. Choose the PCloud Drive Folder

5. Select in your PCloud directory hierarchy where you want the local folder to sync

6. Click "Save" and the "Add Sync".

The sync will start immediately and will be available to all devices connected with your PCloud account. You can add several sync folders provided you don't run out of space. Note that the

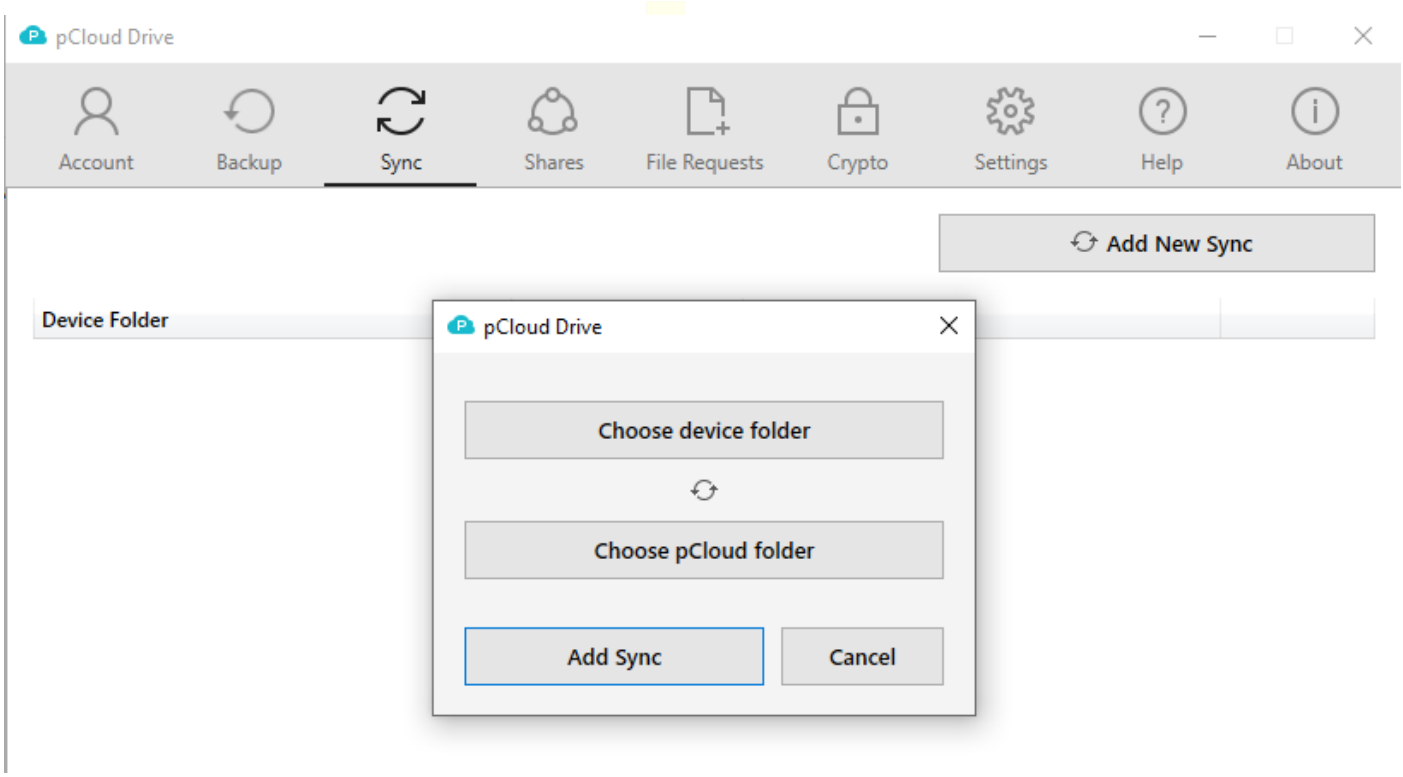


Figure 8 Pcloud Sync Setting

Synchronization process makes your folders available even in offline mode if you choose to do

So just right-click on the folder and click "Offline Access (Sync)".

You can select the PCloud Drive folder or the local folder. Click the "Save" button once you are done with your selection to save the synchronization folder.

12.3 How to upload files through the website

1. Click on the "Upload" icon.
2. Select "File upload" or "Folder upload".
3. Click on "Browse for files" or "Pick folder". Use the "Insert Citation" button to add citations to this document.

4. Find the files or the folder, mark them and click "Open" or "0k".

You can also go for the "Remote upload". This feature allows you to download files directly from the web. Once you have the link to the video, paste it into PCloud and click on the "Upload" button. It is essential to have a preselected "Remote Upload". It downloads the video to your PCloud storage. You can achieve greater speeds of up to 100 megabytes if you have a fast internet them. Fact that you are downloading the file directly from the provider's servers.

12.4 How to upload files through PCloud Drive

Simply drag & drop or copy any file or folder to the PCloud imaginary drive or to a folder that is synced with PCloud.

12.5 How to retrieve your files

It is very simple to get your files back in a situation where you delete. Then they're stored for 15 days in the free version. Deleted files car. Be retrieved for 30 days in the premium versions and up to 365 days with extended file history plans. You can also choose to delete the backups permanently.

12.6 Ease of use

PCloud is available for Mac, Windows, and Linux. It has a simple user interface that makes it easy to use. Simply click on the upload button if you want Io upload something or drag the file inside. It also offers easy file sharing as discussed above. The service offers decent download and upload speeds with a very responsive interface.

12.7 Security and encryption

PCloud uses SSL/TLS encryption to guarantee the safety of the files. It is applied when data from your device is transferred to the cloud servers. It stores your files in more than three server locations to enforce top-notch safety measures

The client-side encryption ensures you only you have the keys for file decryption. Your files are hidden safely from any unauthorized access with PCloud unique client-side encryption. The PCloud Crypto subscription encrypts your most essential files while also protecting your password.

12.8 File versioning

PCloud stores personal files for a specific period so you can always find the previous flies. The 'Revisions' feature allows you to restore previous versions and changes made to specific files if necessary.

Click the gear button to access File Revisions and choose the 'Revision' option. File versions can be kept on the free plan for 15 days and 30 days for users upgrading to Premium, Premium Plus or Lifetime.

PCloud Rewind allows you to go back in time and check your previous version files. You can always browse through your account at a specific date and time in the past. If you removed the shared content accidentally, you can rewind the process to restore or download all non-encrypted files

12.9 How to use PCloud Transfer

PCloud Transfer is a feature you can use to transfer files (up to 5 GB) without making an account with PCloud. Simply add the files, add up to 10 recipient emails, your email and an optional message. The files will then transfer to their servers and will be available to download 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

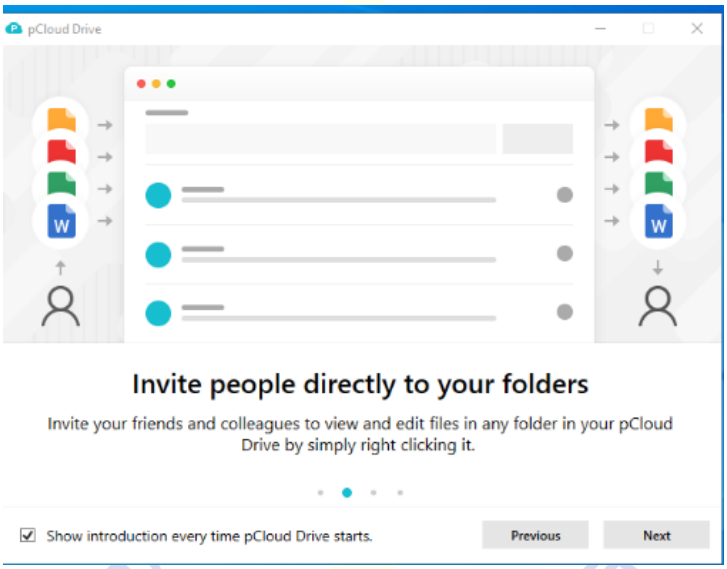


Figure 9 Pcloud Installations

Bydeafult 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

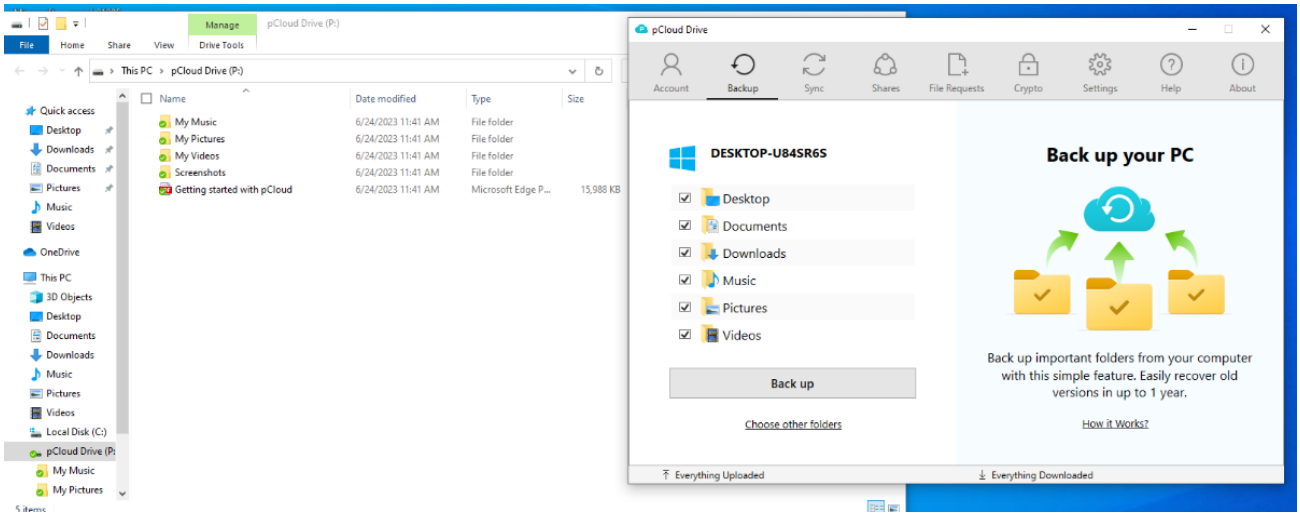


Figure 10 Pcloud Disk Folder

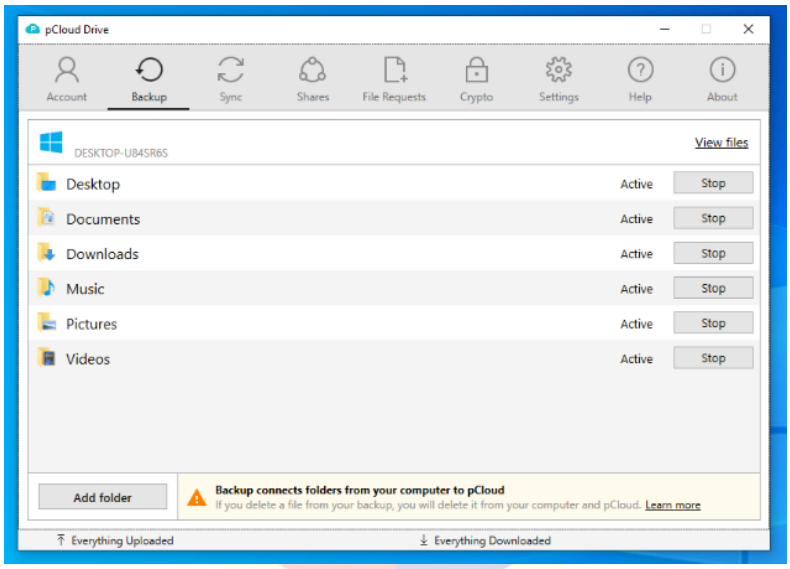


Figure 11 Pcloud Backup Folder Setting

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

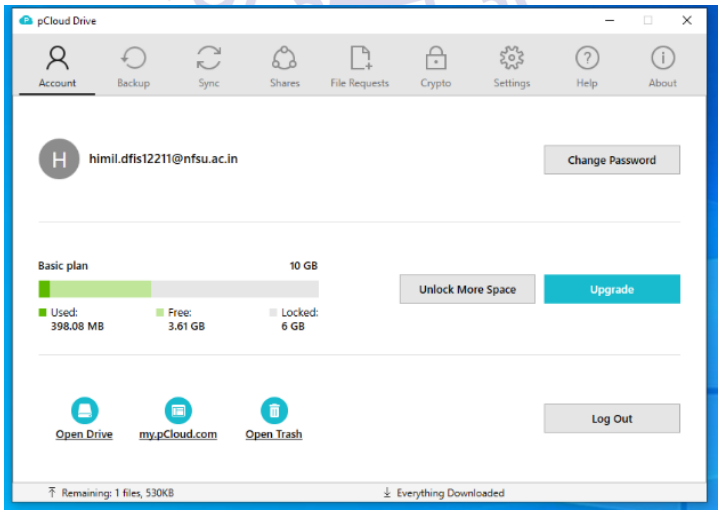


Figure 12 Pcloud 5 GB space Limited Setting

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

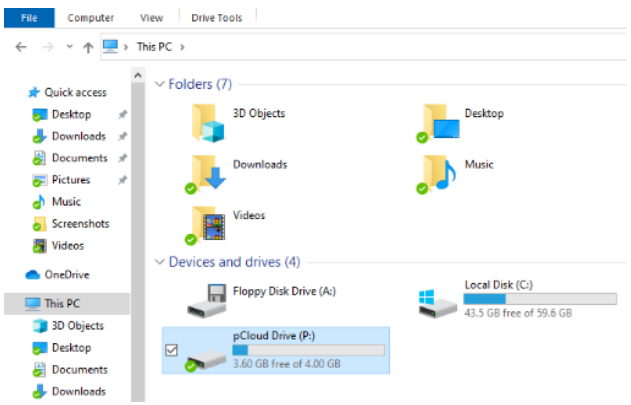


Figure 13 Pcloud Disk available

It`s file extinction exfat

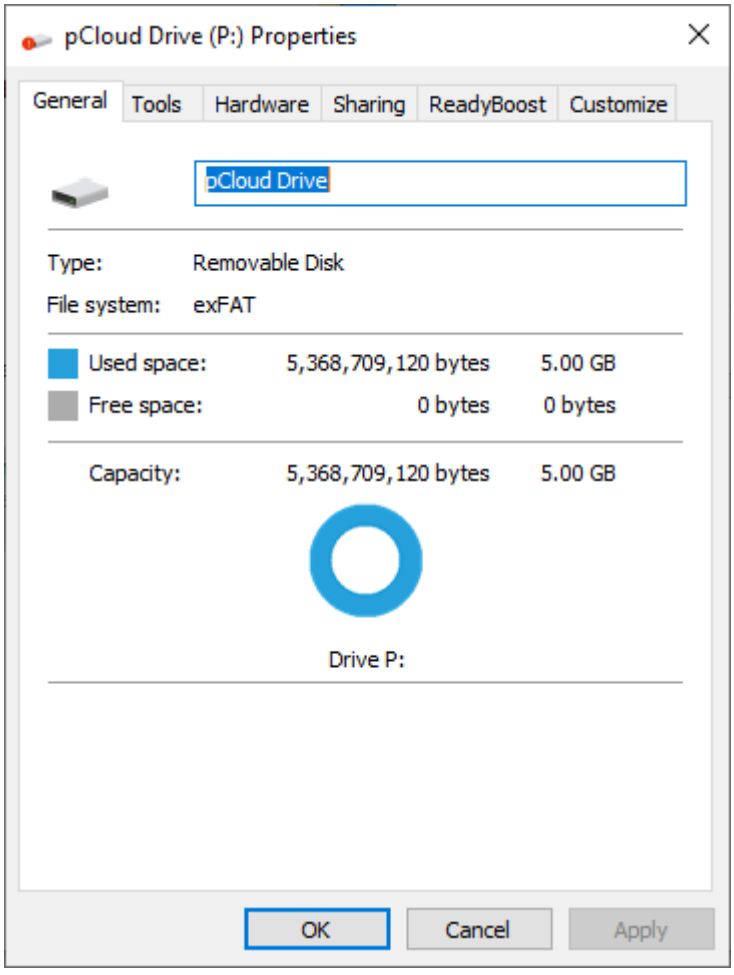


Figure 14 Pcloud Disk Extension

PCloud current version is the 4.1.1

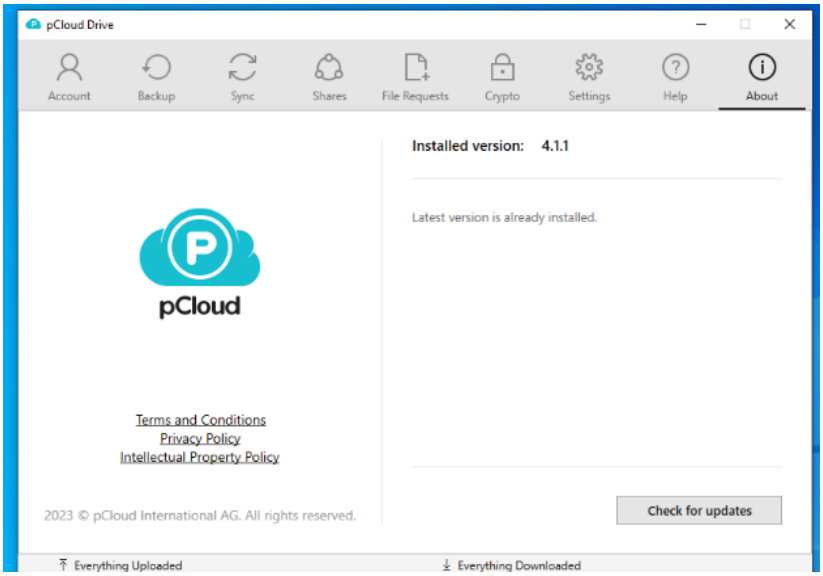


Figure 15Pcloud Version

For the user private data storage crypto 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

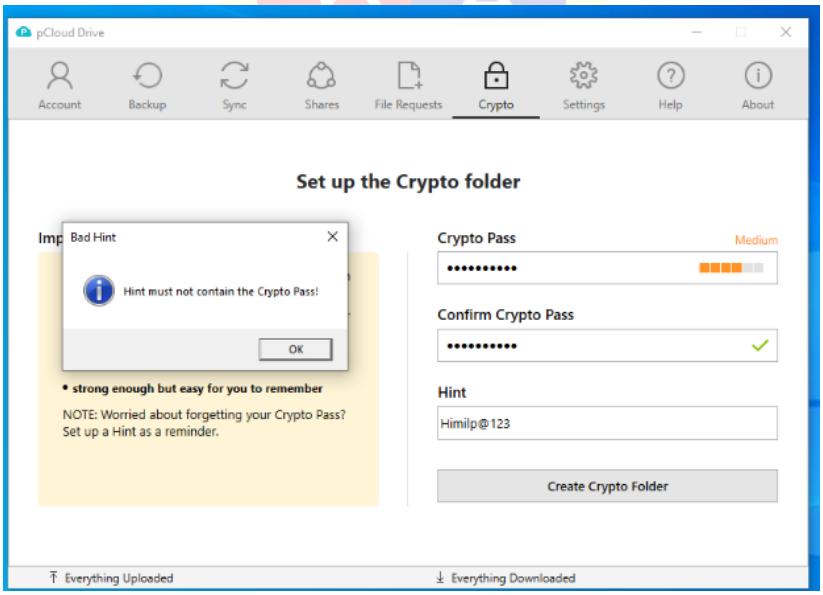


Figure 16 Pcloud Crypto Folder Setting

One drop back is there no password recovery is there

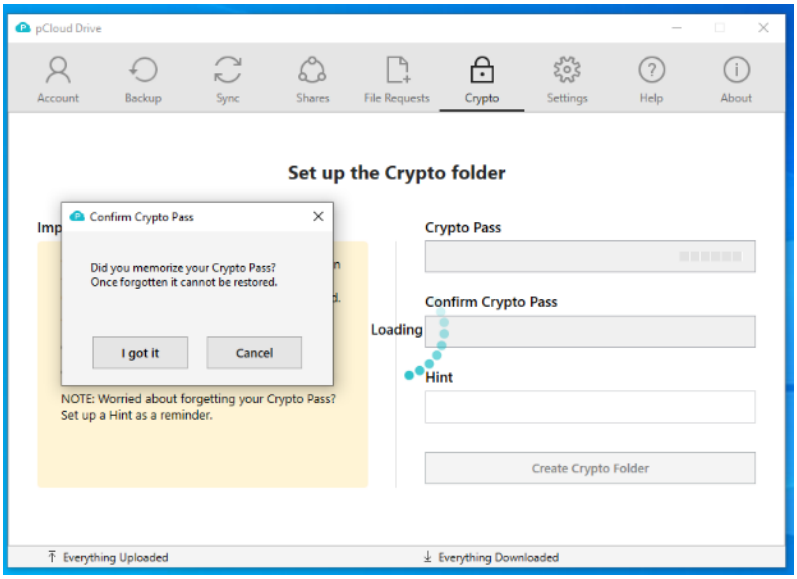


Figure 17 Pcloud Crypto Password not recover

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

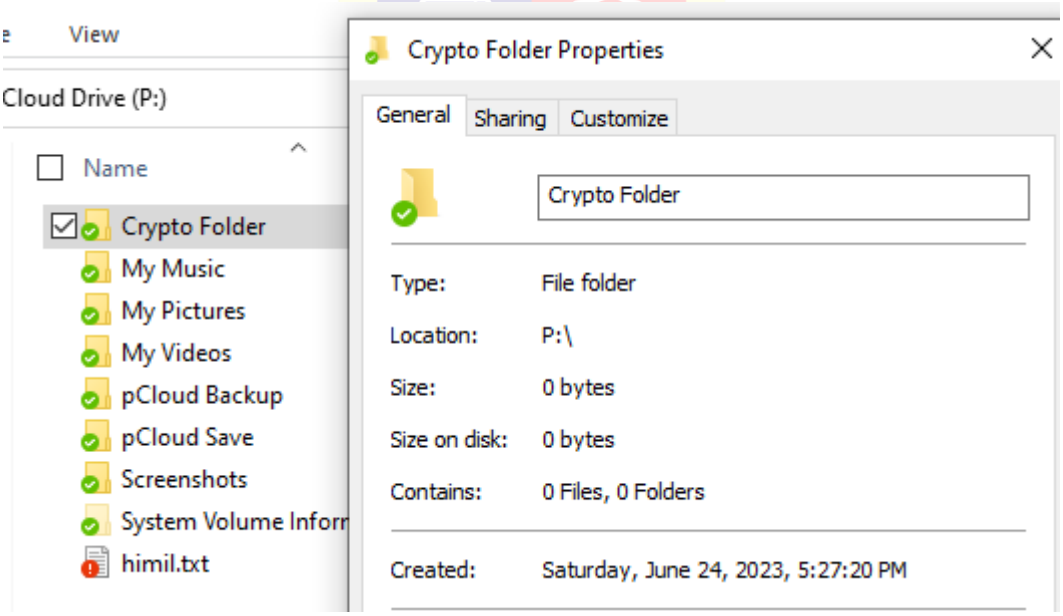


Figure 18 Pcloud Crypto folder empty in lock

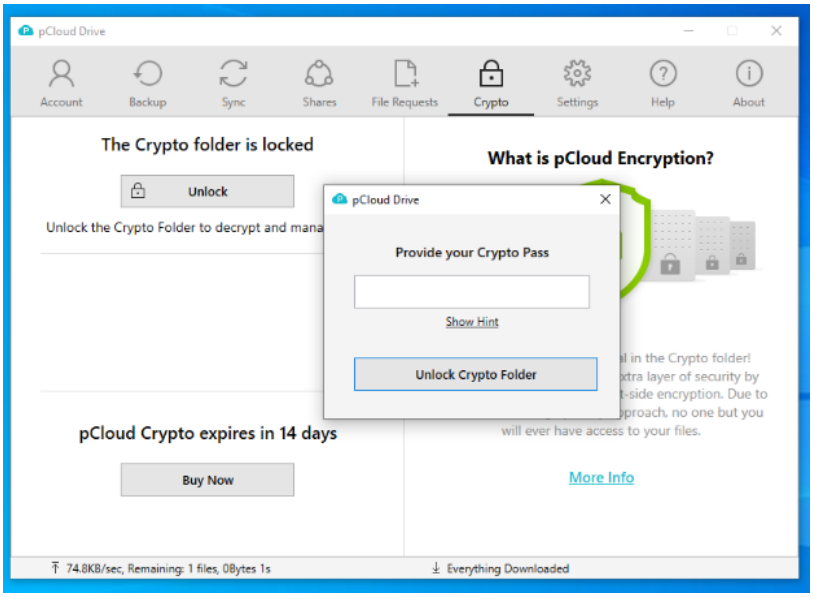


Figure 19 Pcloud crypto folder unlock

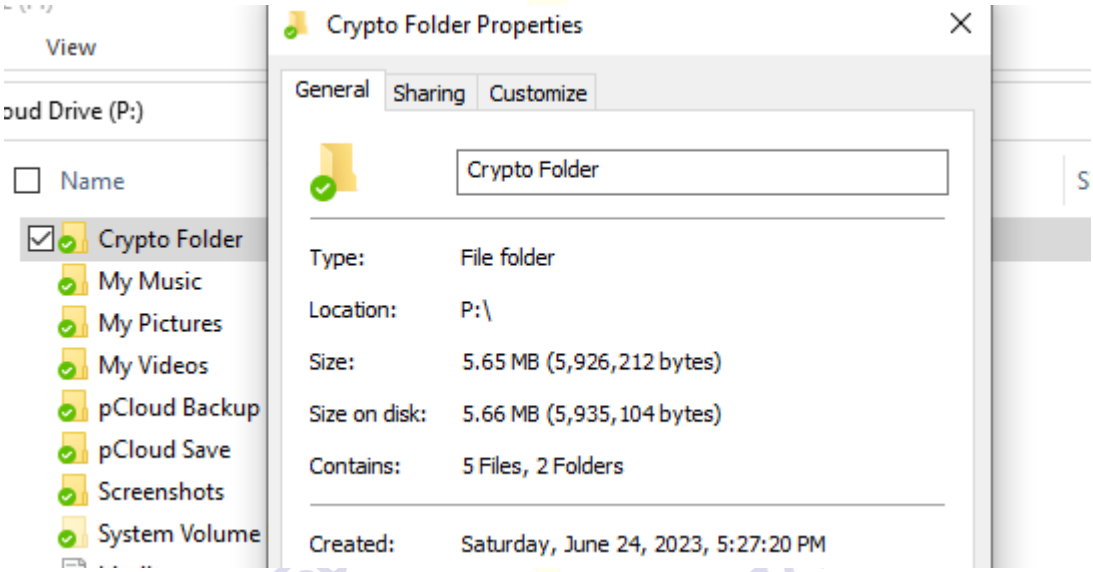


Figure 20Pcloud size shown after unlock

After the install the PCloud extensions in the chrome we can save the image and video in the PCloud directly by the alter key press and just click the image it will save in the PCloud directly no need to download

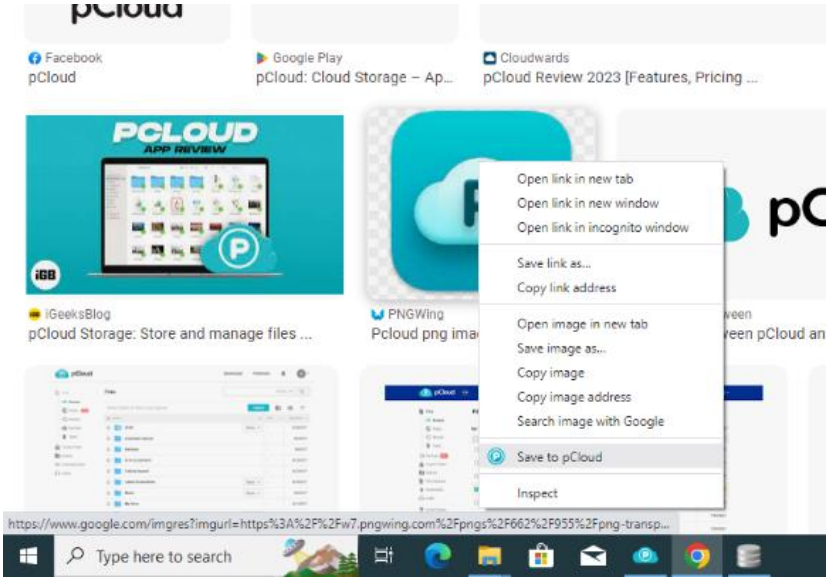


Figure 21 Pcloud Chrome Extensions

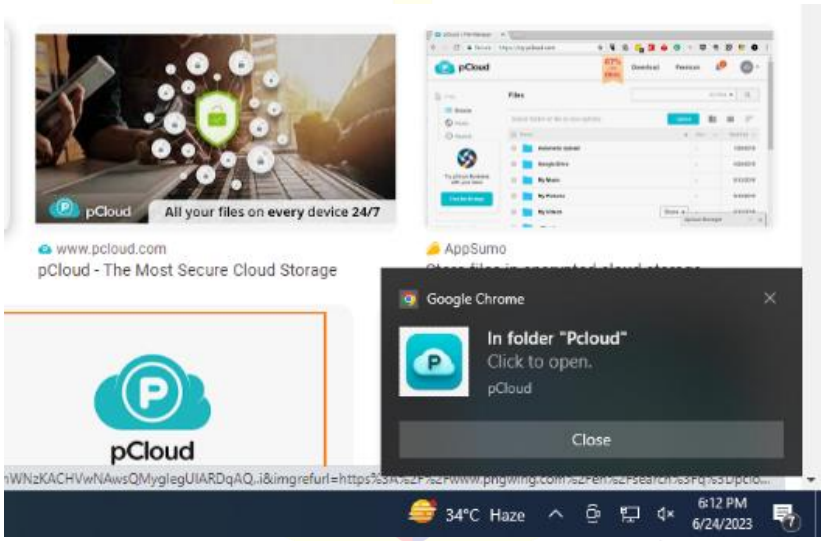


Figure 22Image direct save into Pcloud with extension

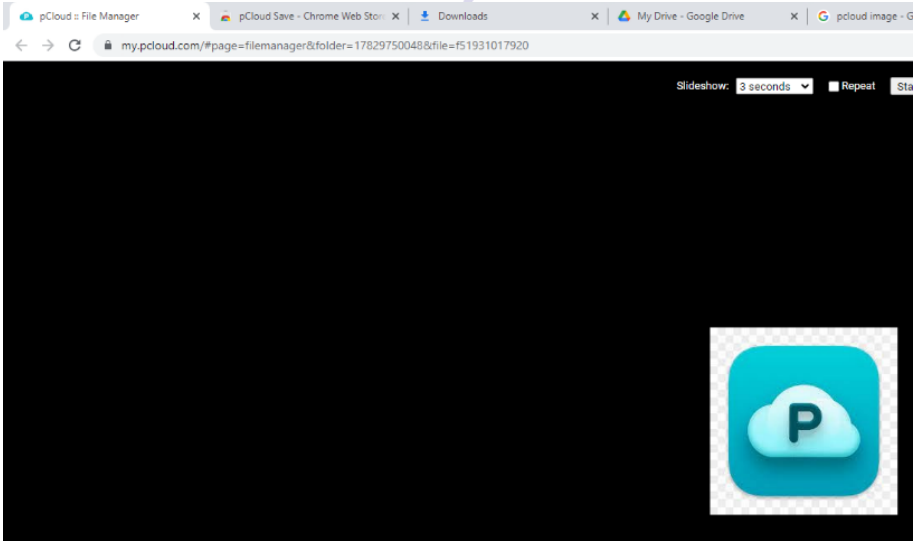


Figure 23image stored in cloud from chrome

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

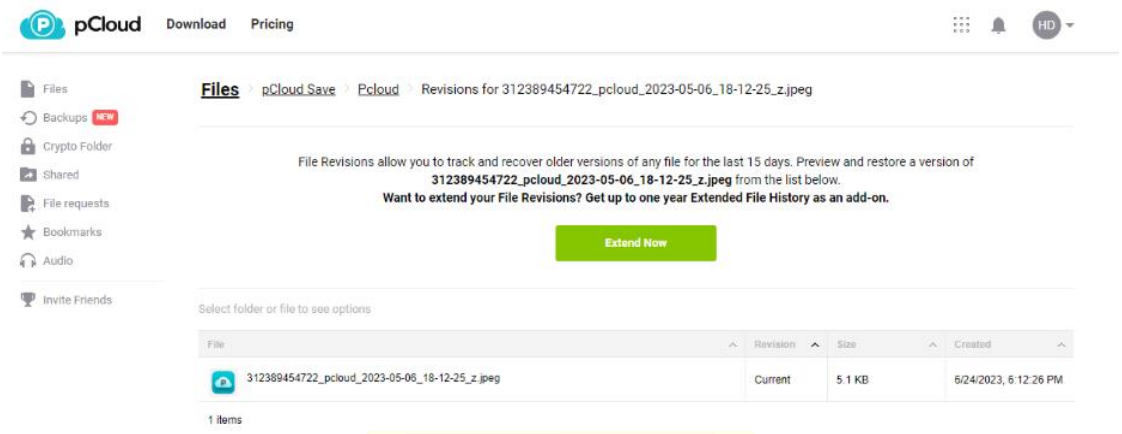


Figure 24Rewind state

12.11 RAM dump

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

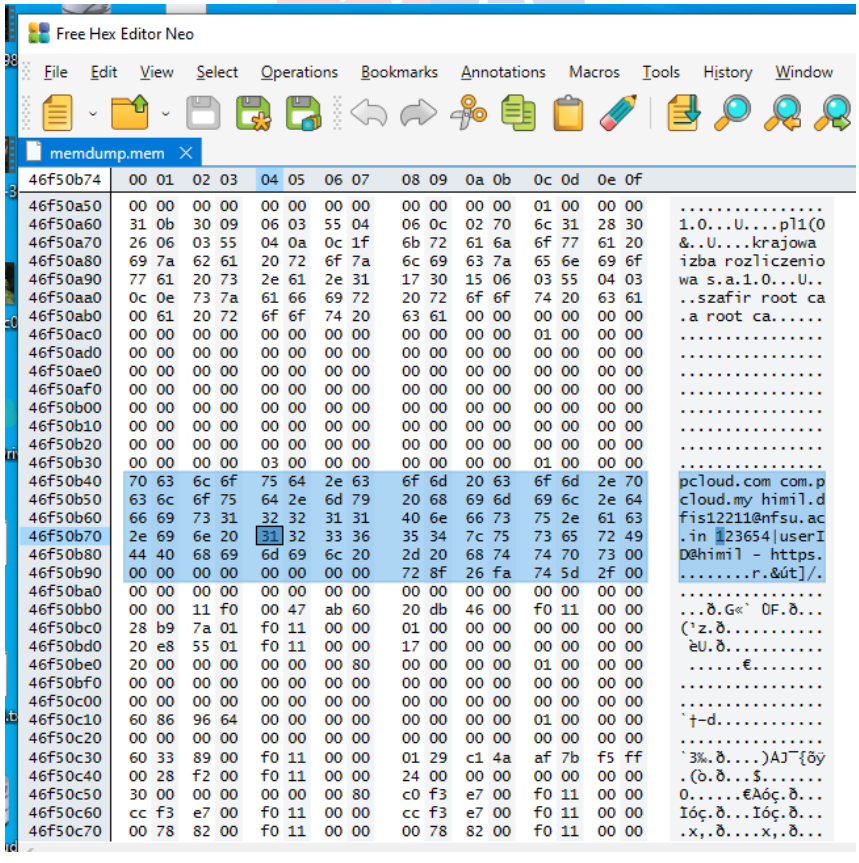


Figure 25Id Password shown in Ram Dump

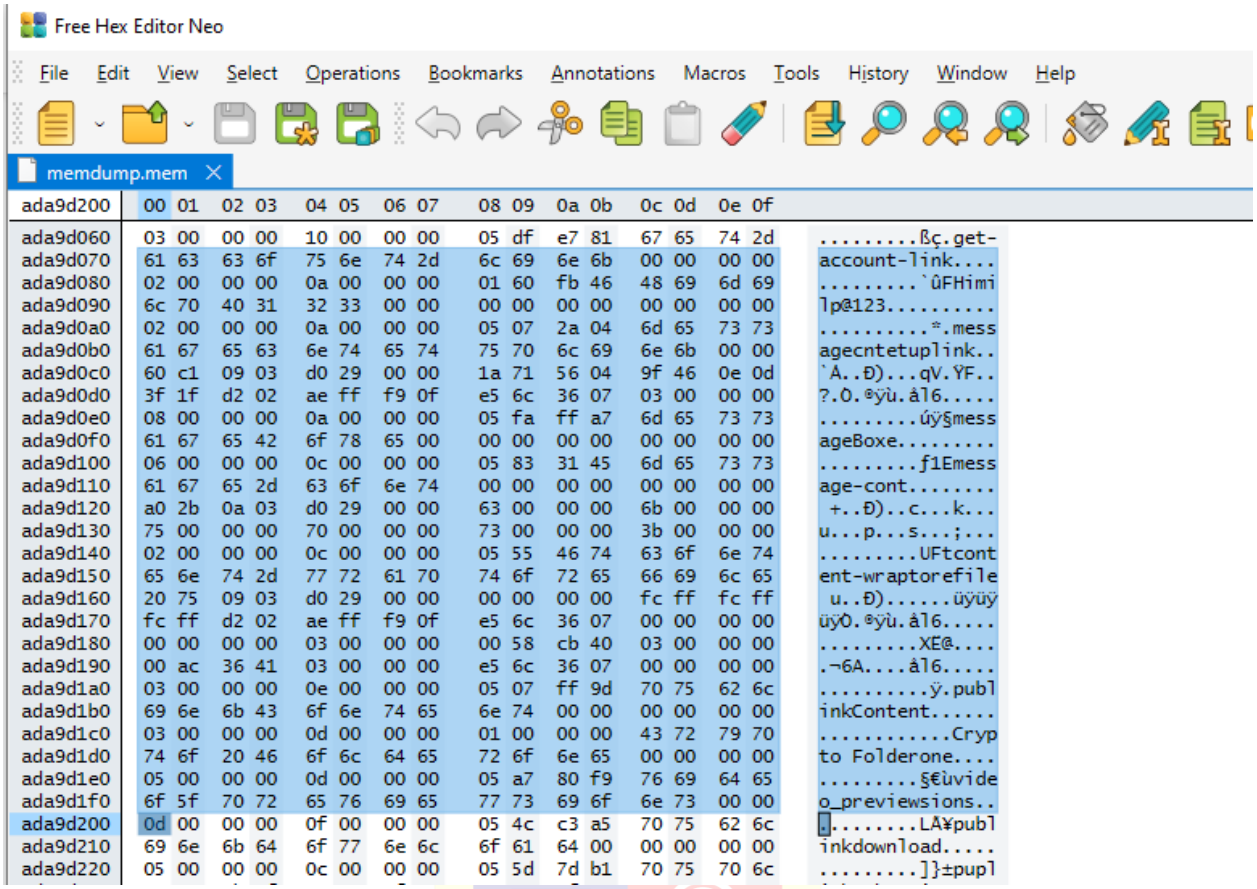


Figure 26Crypto Password reveal in Ram Dump

Crypto folder password found by FTK Ram. DUMP

User id and password find by the FTK RAM. Dump

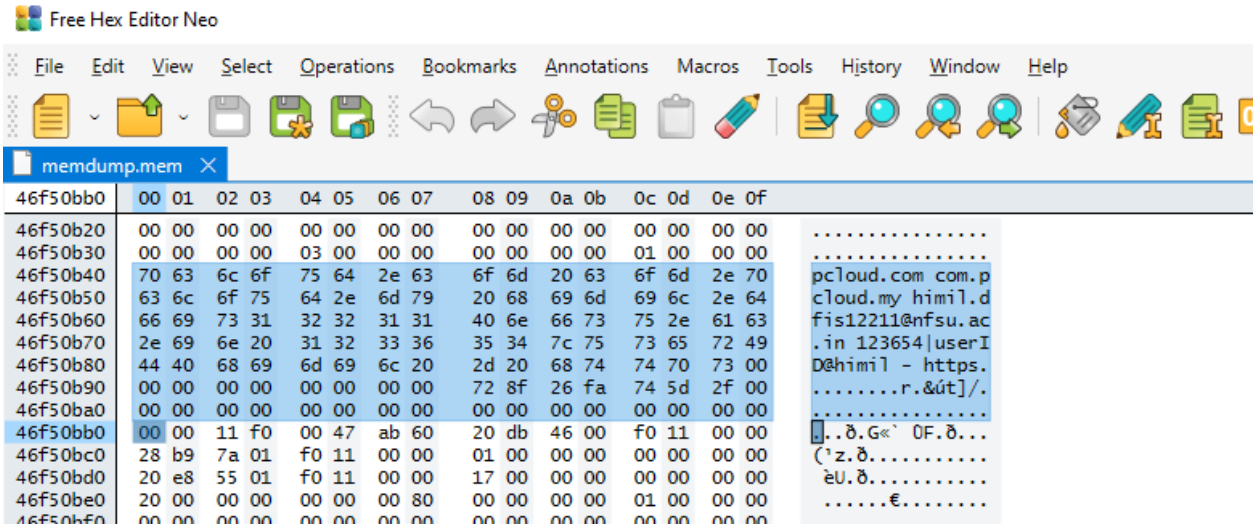


Figure 27File location reveal in RAM dump

DLL FILES FROM the process monitor of Microsoft internal suit

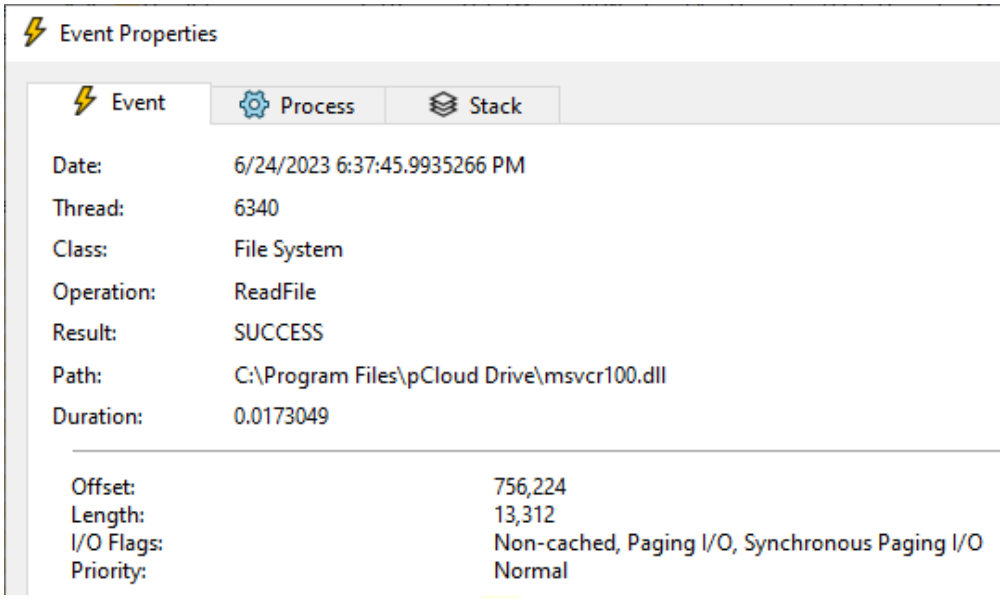


Figure 28msvcr.all used by Pcloud

6:37:45.9935266 PM pCloud.exe 7804 Read File C:\Program Files\PCloud Drive\msvcr100.dll SUCCESS Offset: 756,224, Length: 13,312, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, and Priority: Normal

6:37:46.0117455 PM pCloud.exe 7804 Read File C:\Program Files\PCloud Drive\pthreadVC2.dll SUCCESS Offset: 72,192, Length: 4,608, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, and Priority: Normal

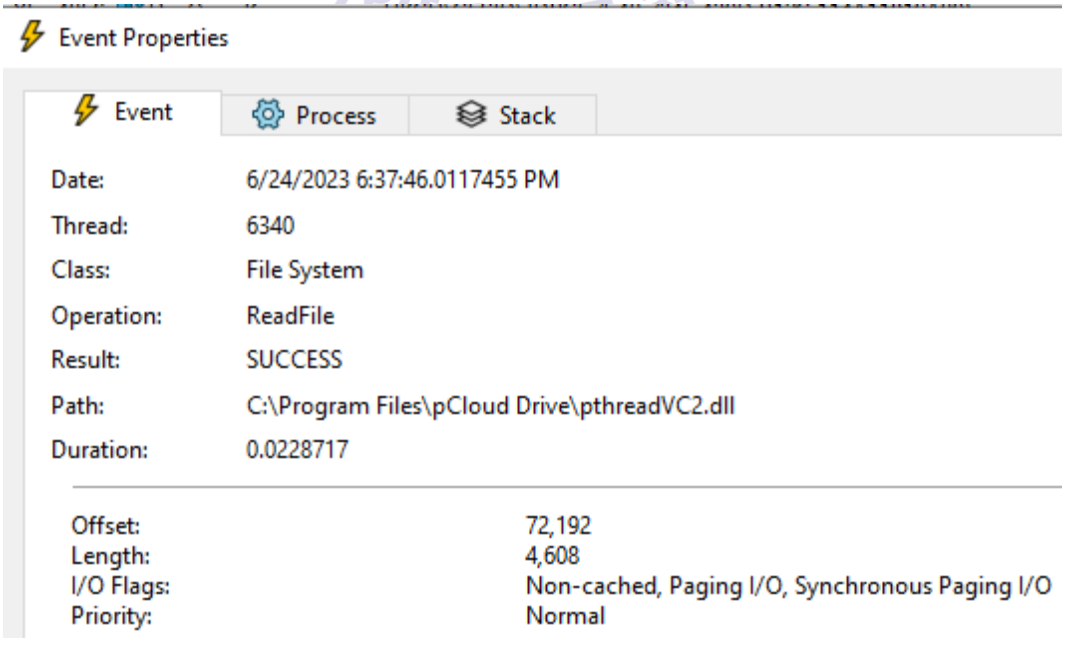


Figure 29 PthreadVC2.dll used by PCloud

6:37:46.0352154 PM pCloud.exe 7804 Read File C:\Program Files\PCloud Drive\pSyncLib.dll SUCCESS Offset: 2,338,304, Length: 14,336, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, and Priority: Normal

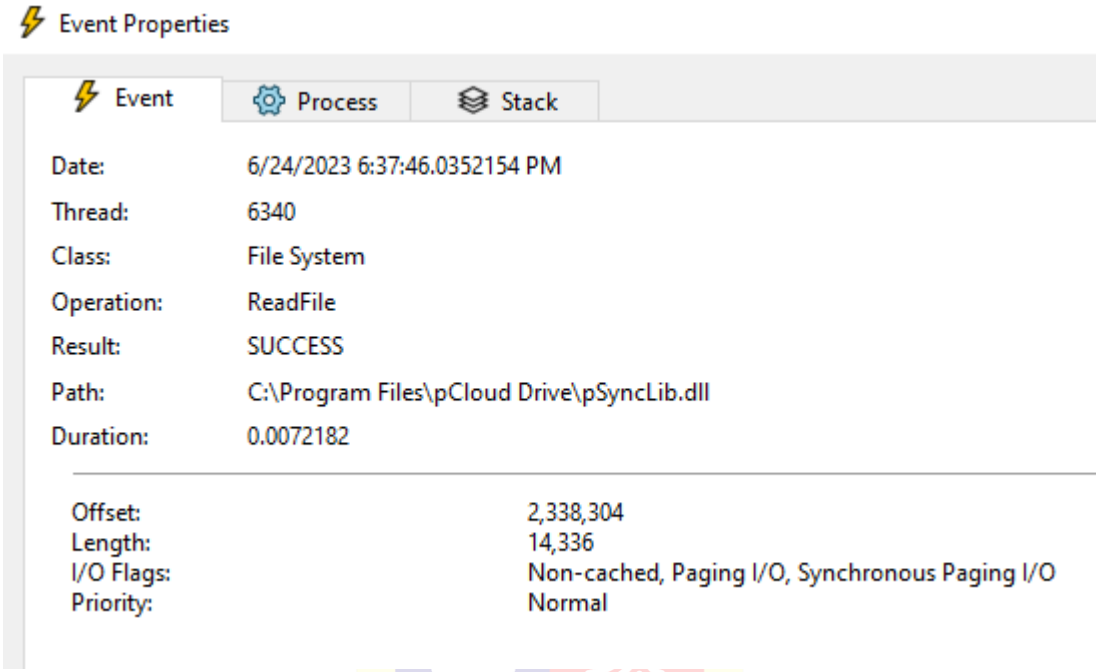


Figure 30 Psynclib.dll used by the Pcloud

6:37:46.0548828 PM pCloud.exe 7804 Thread Create SUCCESS Thread ID: 4196

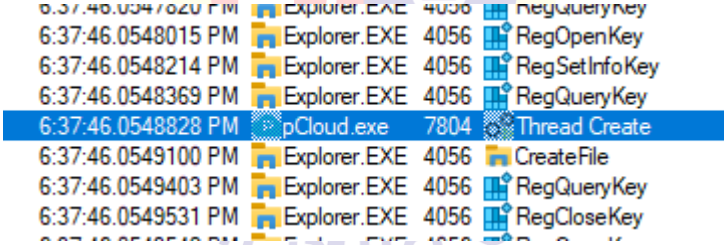


Figure 31Threat created by the PCloud process

6:37:46.0831134 PM pCloud.exe 7804 Thread Exit SUCCESS Thread ID: 5084, User Time: 0.0000000, Kernel Time: 0.0000000

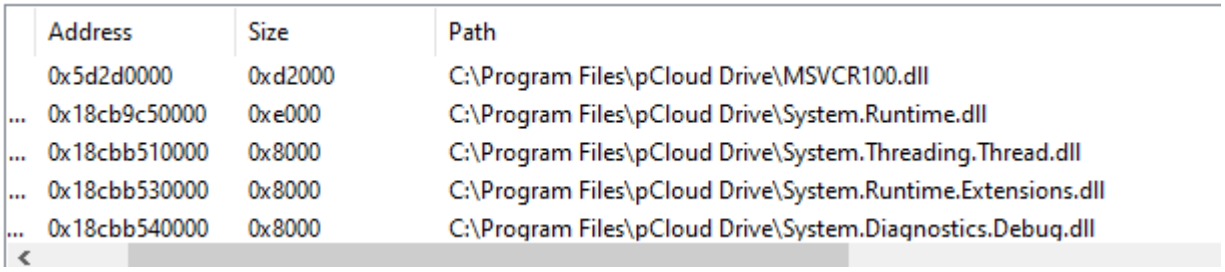


Figure 32List of all Dll used by Pcloud

12.12 Disk analyses

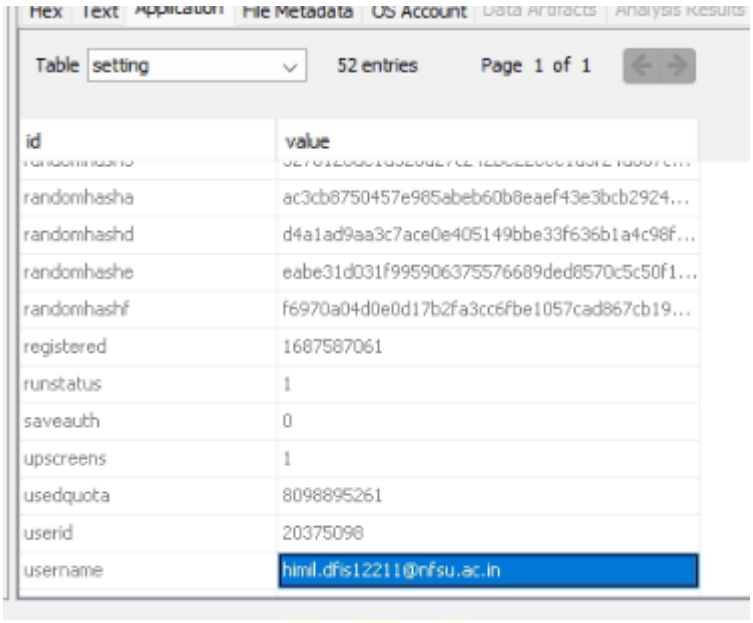


Figure 33Pcloud DB find used id

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

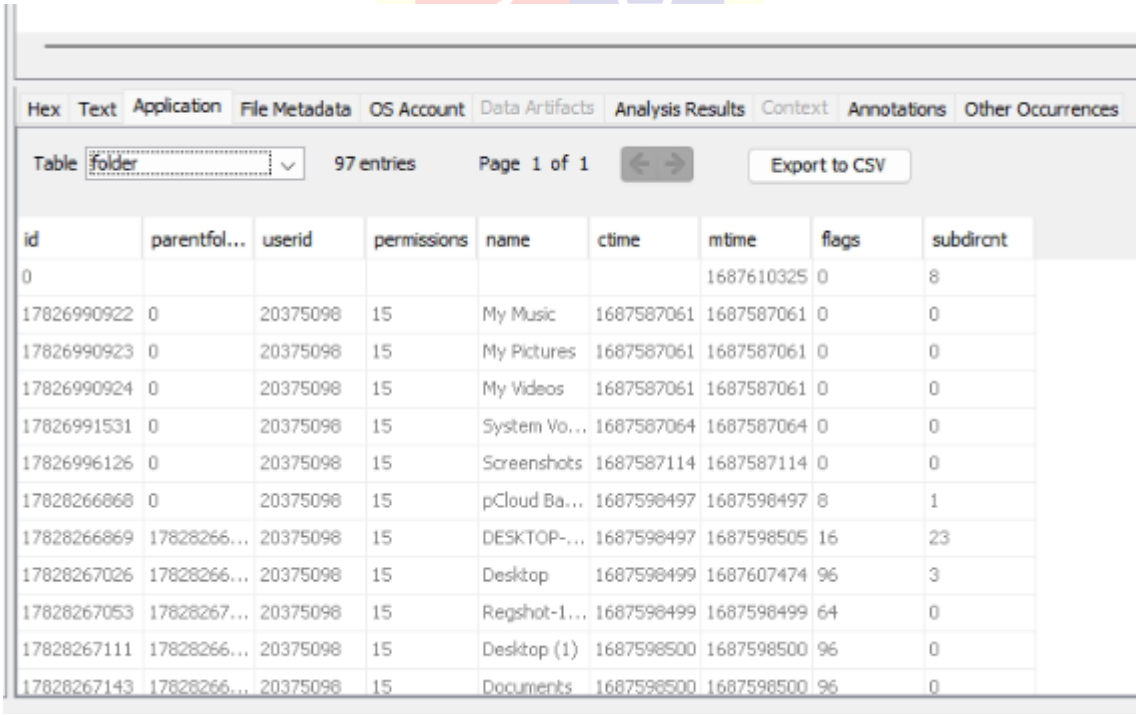


Figure 34 List of all Folder sync with PCloud

Name	S	C	O	Modified Time	Change Time	Acc
[current folder]				2023-06-24 15:53:48 IST	2023-06-24 17:42:29 IST	202
[parent folder]				2023-06-25 17:10:46 IST	2023-06-25 17:10:46 IST	202
Cache				2023-06-25 12:22:28 IST	2023-06-25 12:22:28 IST	202
EBWebView				2023-06-25 17:47:18 IST	2023-06-25 17:47:18 IST	202
ntfthumbs				2023-06-24 11:38:16 IST	2023-06-24 11:38:16 IST	202
data.db	▽		0	2023-06-25 17:43:39 IST	2023-06-25 17:43:39 IST	202
data.db-shm			0	2023-06-25 17:42:54 IST	2023-06-25 17:42:54 IST	202
data.db-wal	▽		0	2023-06-25 17:46:00 IST	2023-06-25 17:46:00 IST	202
wpflog.log	▽		0	2023-06-25 17:43:39 IST	2023-06-25 17:43:39 IST	202

Figure 35 Pcloud DB Folder

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

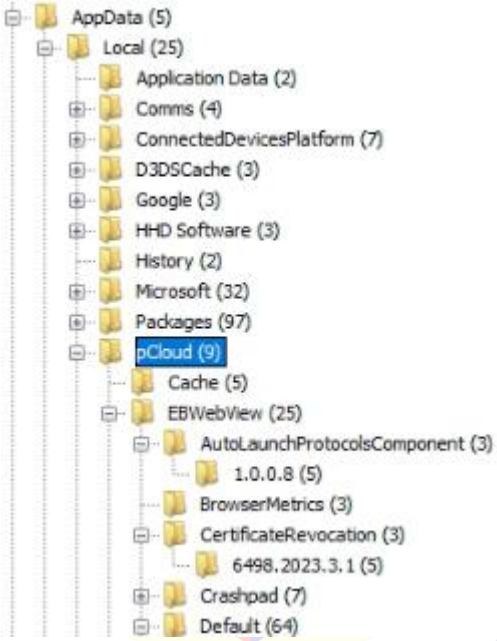


Figure 36 Pcloud Hidden Folder

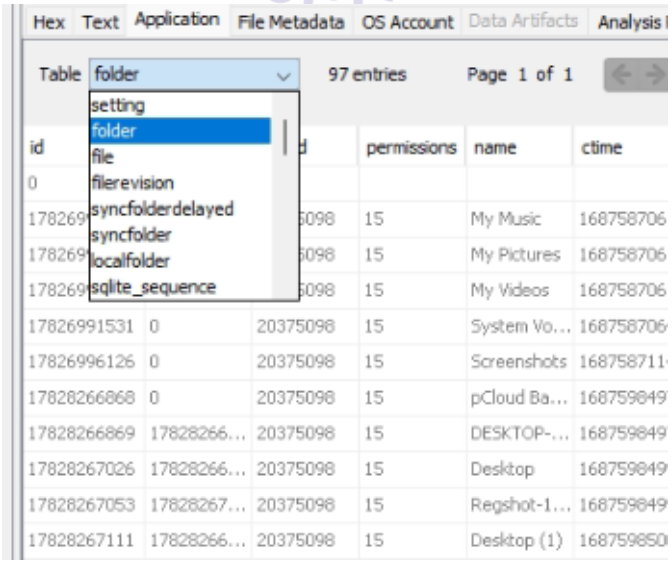


Figure 37Pcloud DB Table

Table file 696 entries Page 1 of 7 Export to CSV

id	parentfolderid	userid	size	hash	flags	name
51923320893	17826990922	20375098	1442376	3954025615383849774	0	Demo Audio 2.mp3
51923320895	17826990922	20375098	6698872	-7922415411591034935	0	GotJoy.mp3
51923320897	17826990922	20375098	28096964	-6556302459936115408	0	Lovely Day.wav
51923320898	17826990922	20375098	11252576	7442273976553368088	0	Momentum.mp3
51923320899	17826990923	20375098	666846	5573129726978457331	0	friends.jpg
51923320900	17826990923	20375098	189628	4167953113435779484	0	happy-family.jpg
51923320901	17826990923	20375098	32905	872630083993397953	0	in-the-sky.jpg
51923320902	17826990923	20375098	500130	4440263624527655250	0	lovers.jpg
51923320903	17826990923	20375098	238222	-8269308721098627382	0	romance.jpg
51923320904	17826990923	20375098	162388	-3267656186046566473	0	sweet.jpg
51923320905	17826990924	20375098	6319438	6446287496907714112	0	pCloud.mp4
51923323762	17826991531	20375098	12	1806630700463301397	0	WPSettings.dat

Figure 38 Pcloud Files Sync List

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

Table syncfolder 6 entries Page 1 of 1 Export to CSV

id	folderid	localpath	synctype	flags	inode	deviceid
1	17828267026	C:\Users\PCLOUD\Desktop	7	1	562949953542262	3193454187
2	17828267143	C:\Users\PCLOUD\Documents	7	1	562949953542261	3193454187
3	17828267248	C:\Users\PCLOUD\Downloads	7	1	562949953542260	3193454187
4	17828267405	C:\Users\PCLOUD\Music	7	1	562949953542257	3193454187
5	17828267503	C:\Users\PCLOUD\Pictures	7	1	562949953542256	3193454187
6	17828267621	C:\Users\PCLOUD\Videos	7	1	562949953542254	3193454187

Figure 39 Pcloud Sync Folder Location

edbtmp.log		0	to pCloud! - <himil.dfis12211@
edb00009.log		0	to pCloud! - <himil.dfis12211@
edb00008.log		0	to pCloud! - <himil.dfis12211@
edb.log		0	to pCloud! - <himil.dfis12211@
data_1__a3011024		1	"email": "<himil.dfis12211@nfs
data_1__a30100f8		0	"email": "<himil.dfis12211@nfs
data_1__a30100c0		1	"email": "<himil.dfis12211@nfs
data_1__a0011233		0	"email": "<himil.dfis12211@nfs
data_1__a0010e72		0	"email": "<himil.dfis12211@nfs
data_1		0	"email": "<himil.dfis12211@nfs

Figure 40Pcloud Log Files

We find all the data are there in the PCloud drive deleted and not deleted data are there

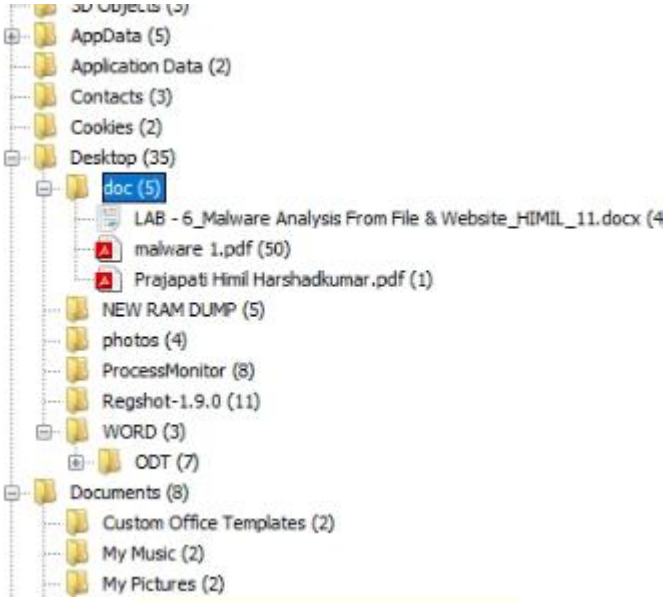


Figure 41Desktop All Files and Folder in Pcloud

12.13 Browser data artifact

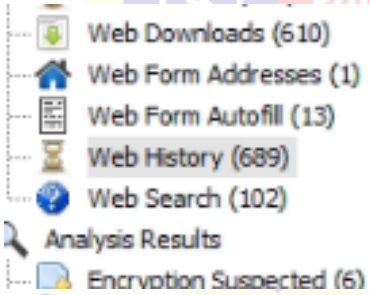
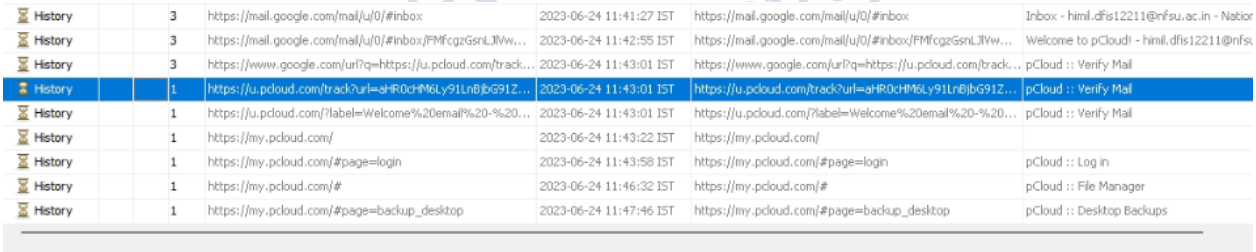


Figure 42 Total Browser History Found



History		3	https://mail.google.com/mail/u/0/#inbox	2023-06-24 11:41:27 IST	https://mail.google.com/mail/u/0/#inbox	Inbox - himil.dfis12211@nfsu.ac.in - Natior
History		3	https://mail.google.com/mail/u/0/#inbox/FMfcgzGsnLJlVw...	2023-06-24 11:42:55 IST	https://mail.google.com/mail/u/0/#inbox/FMfcgzGsnLJlVw...	Welcome to pCloud! - himil.dfis12211@nfsu
History		3	https://www.google.com/url?q=https://u.pcloud.com/track...	2023-06-24 11:43:01 IST	https://www.google.com/url?q=https://u.pcloud.com/track...	pCloud :: Verify Mail
History		1	https://u.pcloud.com/track?url=aHR0cHM6Ly91LnBjbG91Z...	2023-06-24 11:43:01 IST	https://u.pcloud.com/track?url=aHR0cHM6Ly91LnBjbG91Z...	pCloud :: Verify Mail
History		1	https://u.pcloud.com/?label=Welcome%20email%20-%20...	2023-06-24 11:43:01 IST	https://u.pcloud.com/?label=Welcome%20email%20-%20...	pCloud :: Verify Mail
History		1	https://my.pcloud.com/	2023-06-24 11:43:22 IST	https://my.pcloud.com/	
History		1	https://my.pcloud.com/#page=login	2023-06-24 11:43:58 IST	https://my.pcloud.com/#page=login	pCloud :: Log in
History		1	https://my.pcloud.com/#	2023-06-24 11:46:32 IST	https://my.pcloud.com/#	pCloud :: File Manager
History		1	https://my.pcloud.com/#page=backup_desktop	2023-06-24 11:47:46 IST	https://my.pcloud.com/#page=backup_desktop	pCloud :: Desktop Backups

Figure 43Browser 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

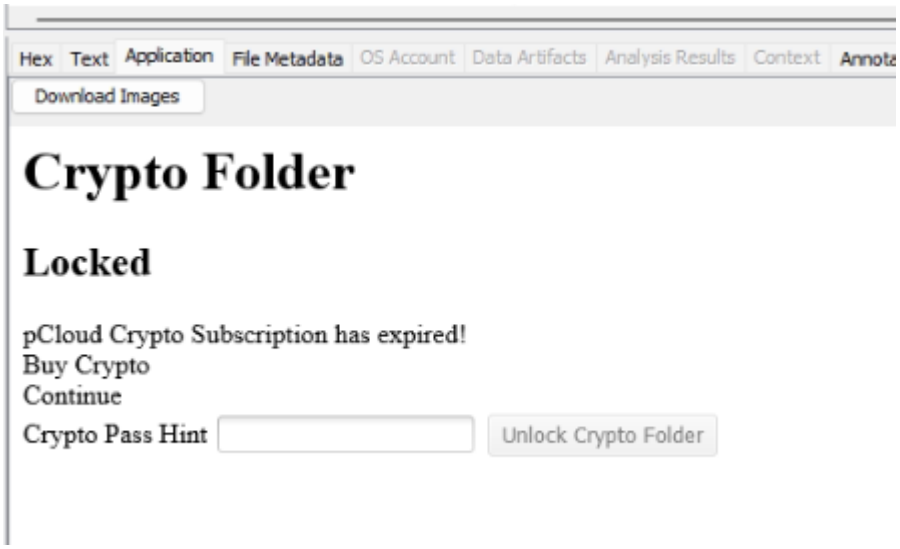


Figure 44 Cache Preview of crypto folder

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

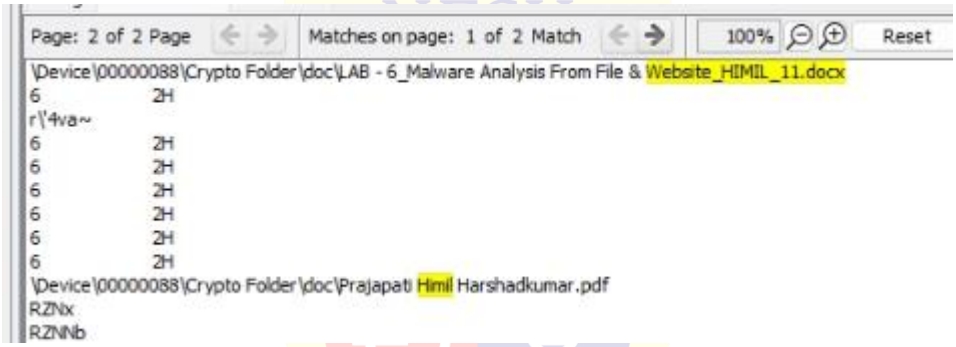


Figure 45Some File name Store in Crypto Folder

We can see the location of the crypto folder in the analysis but in the disk the location is not there we just find the files also that are stored in the crypto folder

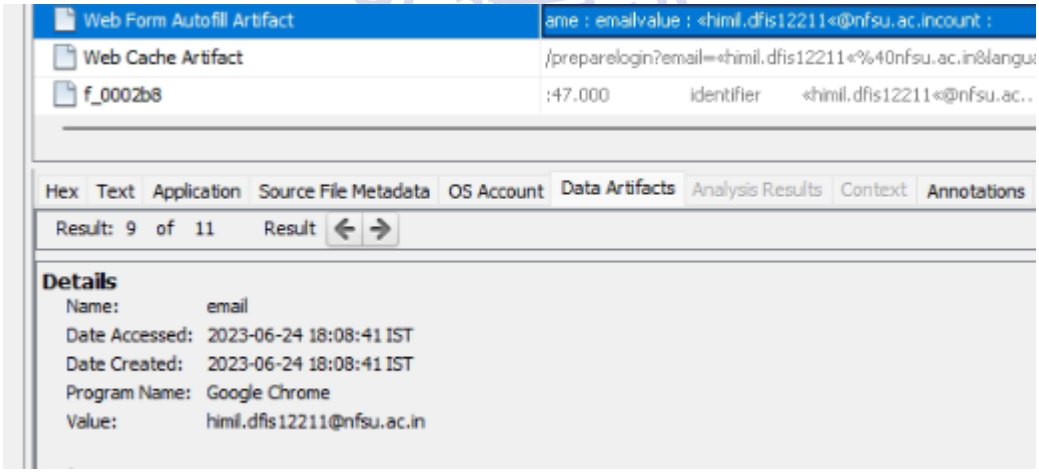


Figure 46 Email id in auto fill means use of the PCloud is more

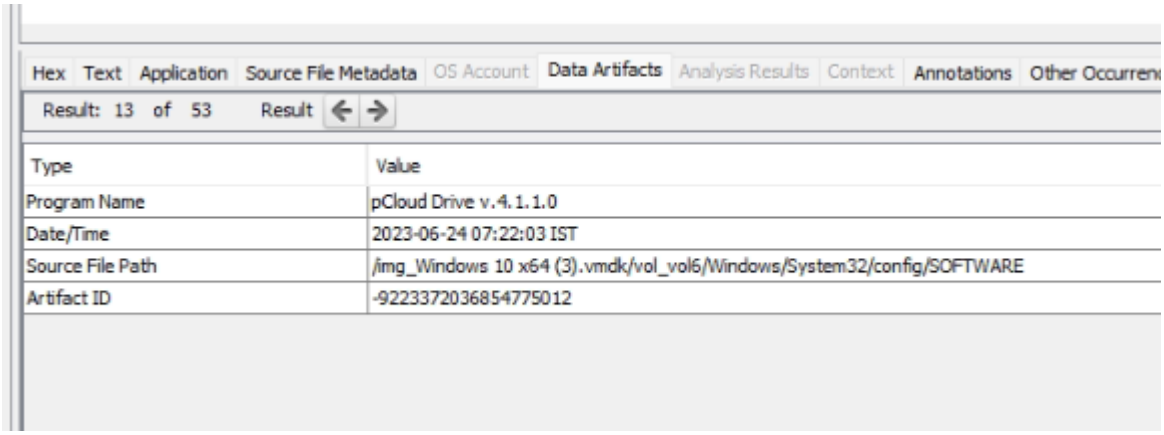


Figure 47Pcloud Version

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

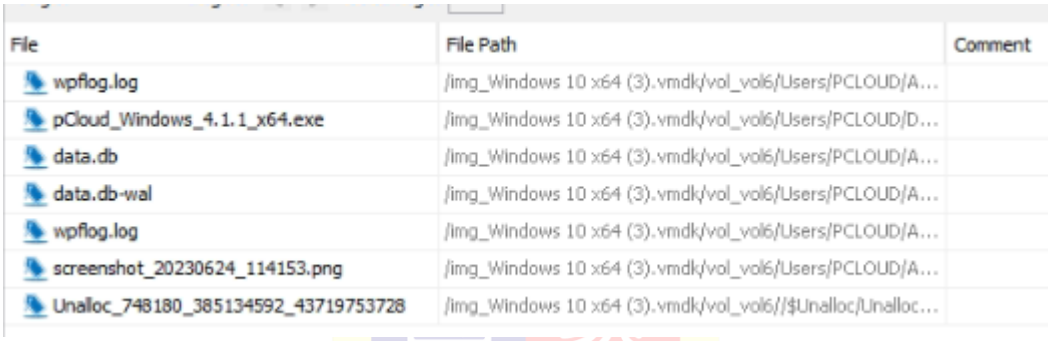


Figure 48List of Bookmark the Evidences

After doing the book mark at to all evidence we can create a report

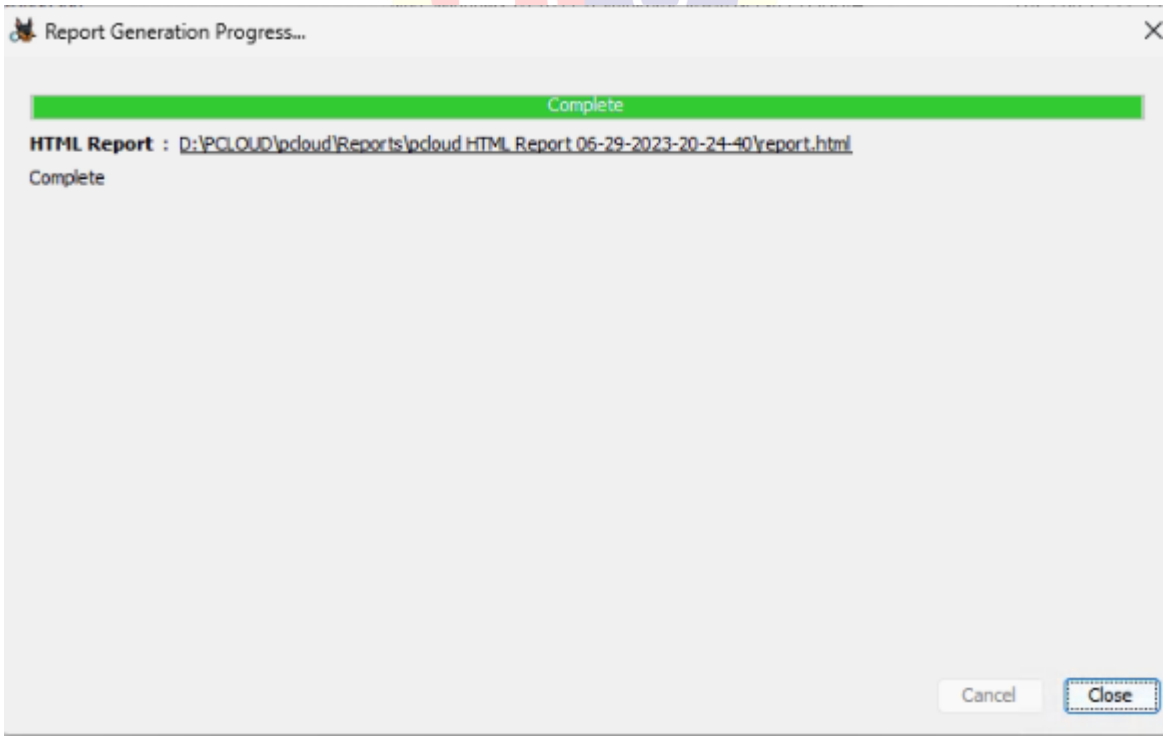


Figure 49Report created by the Autopsy

12.14 Live browser artifact

Installed Extensions

Extension Name	Description	Version	App ID	Profile Folder
Google Docs Offline	Edit, create, and view your documents, spreadsheets, and presentati	1.62.0	ghbmnnjooekpmoecnnnilnnbdlolhkhi	Default
Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	nmmhkkegccagdldgiimedpiccmgmieda	Default
pCloud Save	Save your favorite web images, videos, text and more to pCloud - up	1.5.0	npamdkabjncnnoaofdjcaipmnccofeem	Default

Figure 50Extention installed

20		clear_lso_data_enabled	<not present>
21	Per Host Zoom Levels		
22	Sync Settings		
23		last_poll_time	2023-06-24 12:38:40.422
24		last_synced_time	2023-06-24 13:35:33.022
25		cache_guid	vnAy51H1YT2mVapsreehPA==
26		gaia_id	106807315777188389081
27		requested	FALSE

Figure 51last login status

323	session storage	https://www.pcloud.com/	tt_pixel_session_index	{"index":0}
324	session storage	https://www.pcloud.com/	tt_pixel_session_index	{"index":0}
325	session storage	https://www.pcloud.com/	tt_sessionId	"152b08d6-128f-11ee-89cd-08c0eb5e3f0c::QzuDbGDZTSEVfT7iYRD2"
326	session storage	https://www.pcloud.com/	tt_sessionId	"9cd5a22c-1287-11ee-ad1d-3eb5b6c93e52::OBkgDps4WA26V1KJHGGL"
327	session storage	https://www.pcloud.com/	tt_sessionId	"f2c292d5-128b-11ee-b4a1-a68fb7e4edf5::of3PESJCjEsGCOccJJGN"
328	local storage	https://www.varonis.com	_uetsid	78535540128511eea88507186e4d5f14
329	local storage	https://www.varonis.com	_uetsid_exp	Sun, 25 Jun 2023 11:54:31 GMT
330	local storage	https://www.varonis.com	uetvid	78537a50128511ee841785002e247d64

Figure 52session of pcloud

558	site setting (modif	2023-06-24 05:04:35.617	https://my.pcloud.com:443,*	formfill_metadata [in Prefer
559	url	2023-06-24 05:04:35.808	https://my.pcloud.com/#page=filemanager&crypto=1	pCloud :: File Manager
560	login (never save)	2023-06-24 05:04:40.179	https://my.pcloud.com/	
561	url	2023-06-24 05:05:18.191	https://my.pcloud.com/#page=filemanager&folder=17829463263&tp	pCloud :: File Manager
562	download	2023-06-24 05:05:22.416	blob:https://my.pcloud.com/8dc67b83-ddf1-4fee-ad69-91b0d37cd9a	Complete - 100% [26018/260
563	url	2023-06-24 05:06:02.961	https://my.pcloud.com/#page=filemanager&tpl=folderlist	pCloud :: File Manager

Figure 53login status

13. Mega sync

Mega sync is an intuitive software evolved via mega created Newlands that permits you to effortlessly synchronize folders on numerous computer systems. You honestly need to upload information in the cloud and, within seconds, you may explore the same documents to your drive

You can choose to synchronize your entire MEGA account or configure multiple selective syncs between folders on your computer and folders in your MEGA account. MEGA sync moves deleted files to special folders on your local computer and in your MEGA account so they can be restored if you need to. MegaSyn securely interacts with your browser, handling MEGA file transfers for enhanced performance.

MEGA was architected around the simple fact that cryptography, for it to be accepted and used, must not interfere with usability. MEGA is fully accessible without prior software installs and remains the only cloud storage provider with browser-based high-performance end-to-end encryption. The only visible signs of the crypto layer operating under MEGA's hood are the entropy collection during signup, the lack of a password reset feature and the novel (and browser-specific) ways file transfers are conducted.

Today, millions of business and personal users rely on MEGA to securely and reliably store and serve petabytes of data and we believe that this success is the result of MEGA's low barrier to entry to a more secure cloud. MegaSyn can be accessed in the browser, desktop Client App mobile and command-line Tool. This makes it an around service available every time anywhere anyhow. The service is available of Windows, mac OS and Linux Operating Systems Mega comes with a free 50GB Disk Space for Free use on Signup.

13.1 Installation process

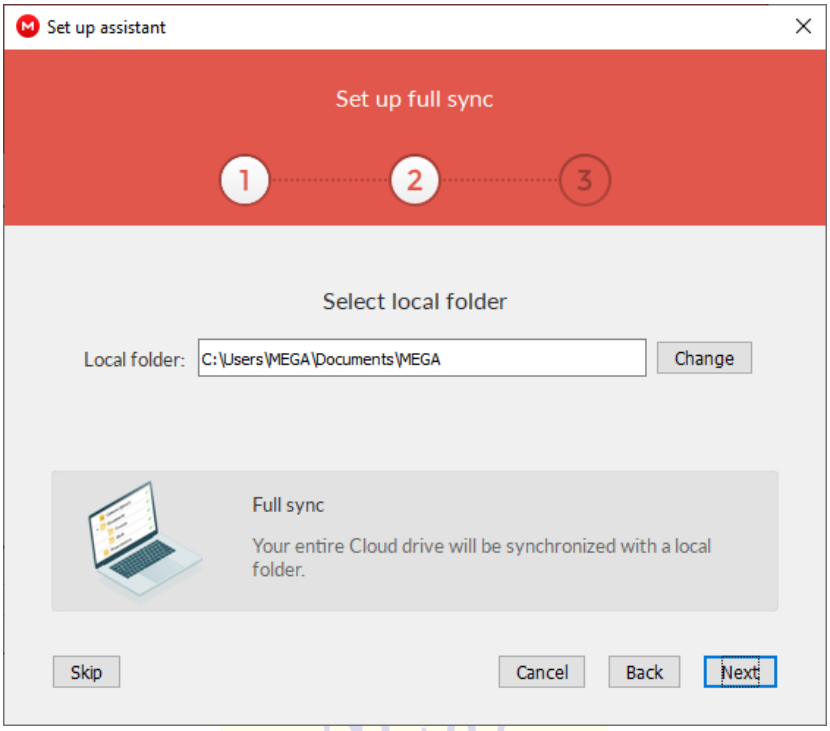


Figure 54 Mega setup Installation

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

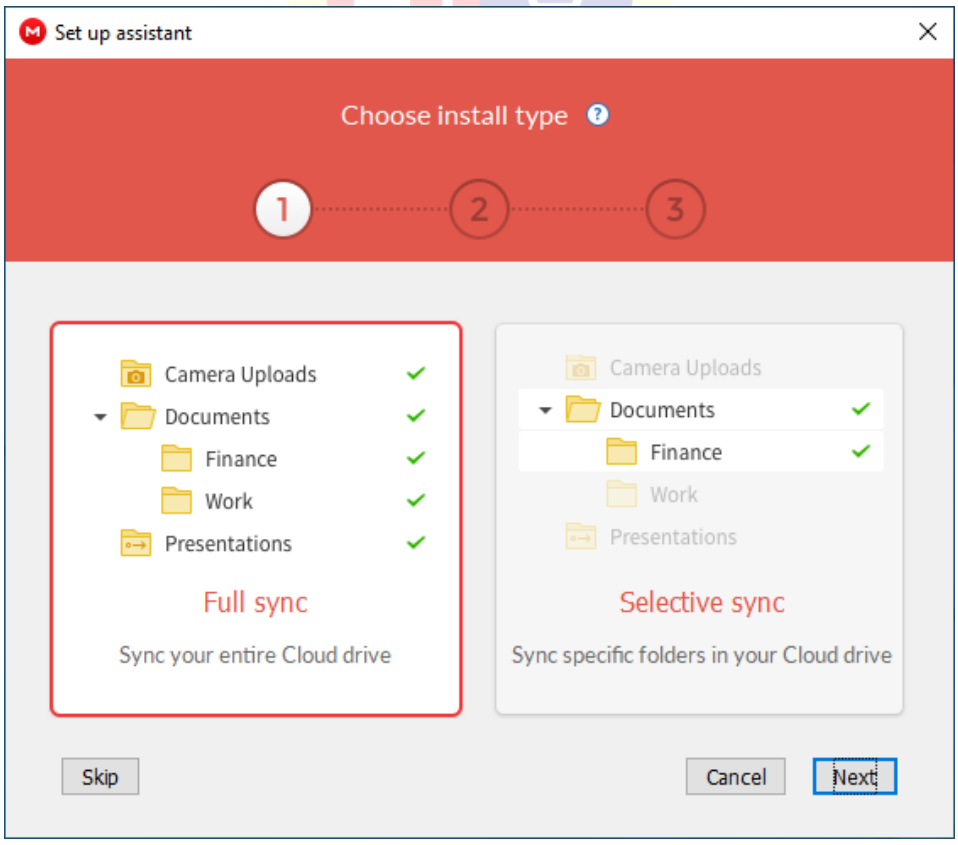


Figure 55 Sync Setting

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

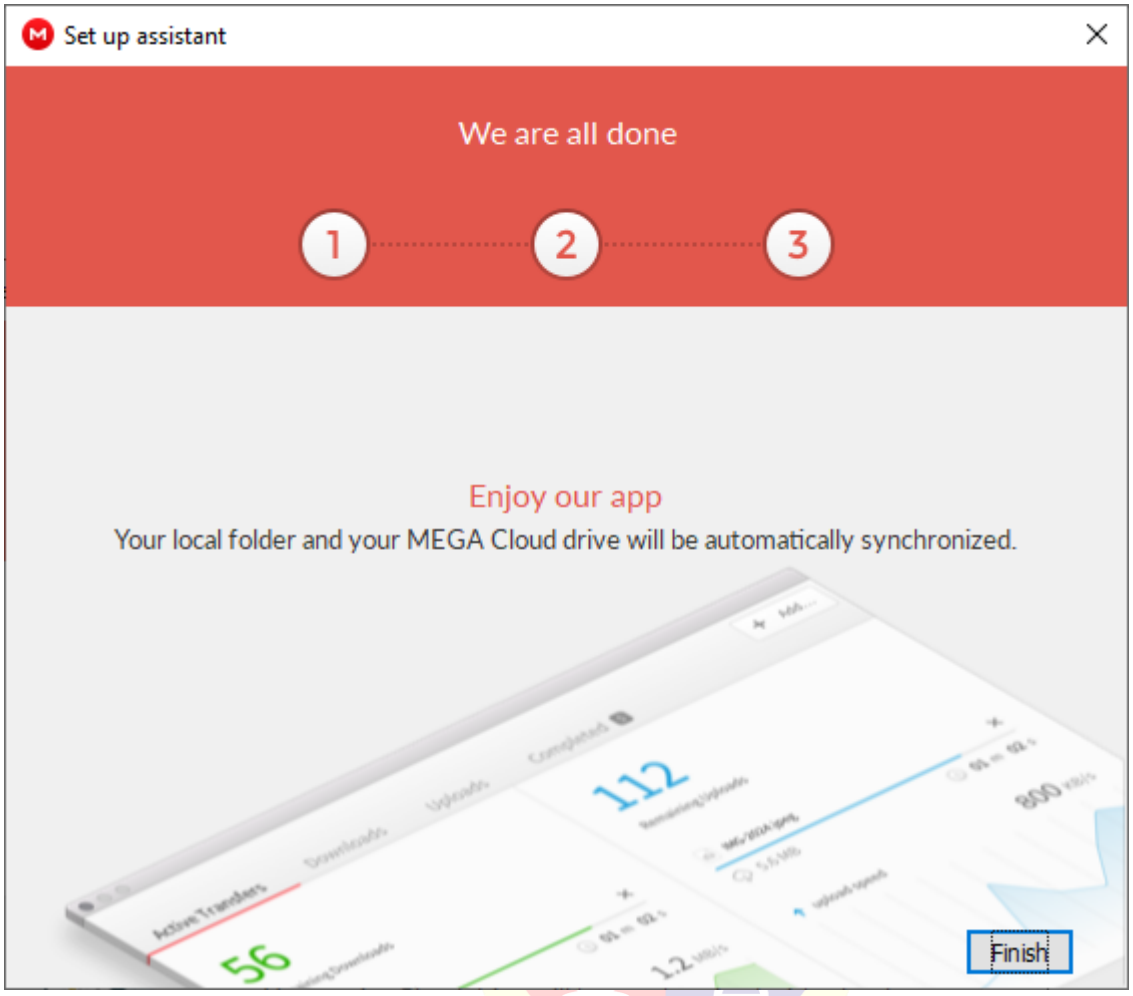


Figure 56 Complete Setup

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

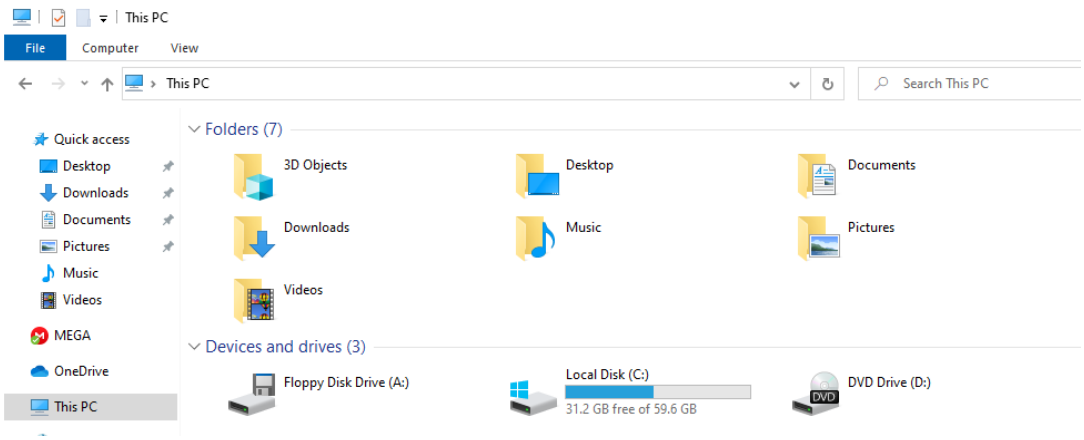


Figure 57 No Local Disk

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 MegaSyn in open for the user interaction

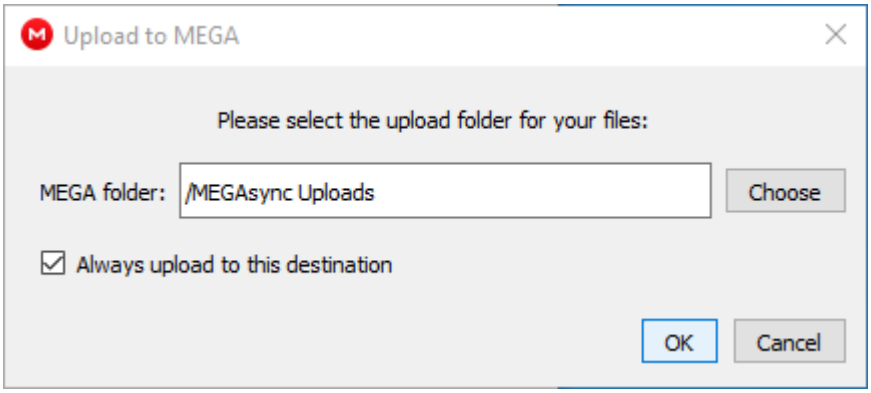


Figure 58 Sync Folder Setting

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

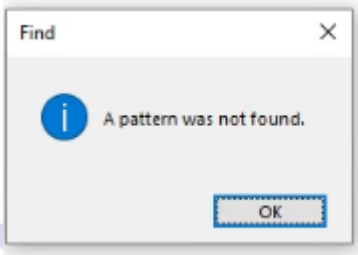


Figure 59 Password not found

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

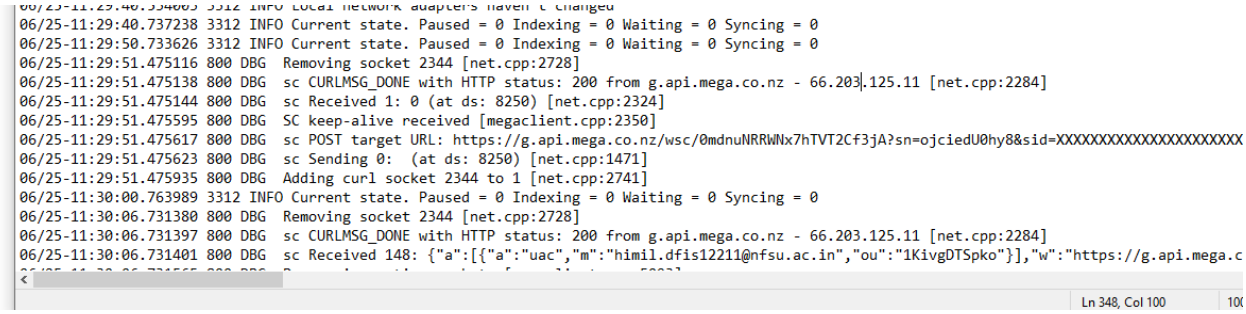


Figure 60 Log Files

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\MegaSyn\logs

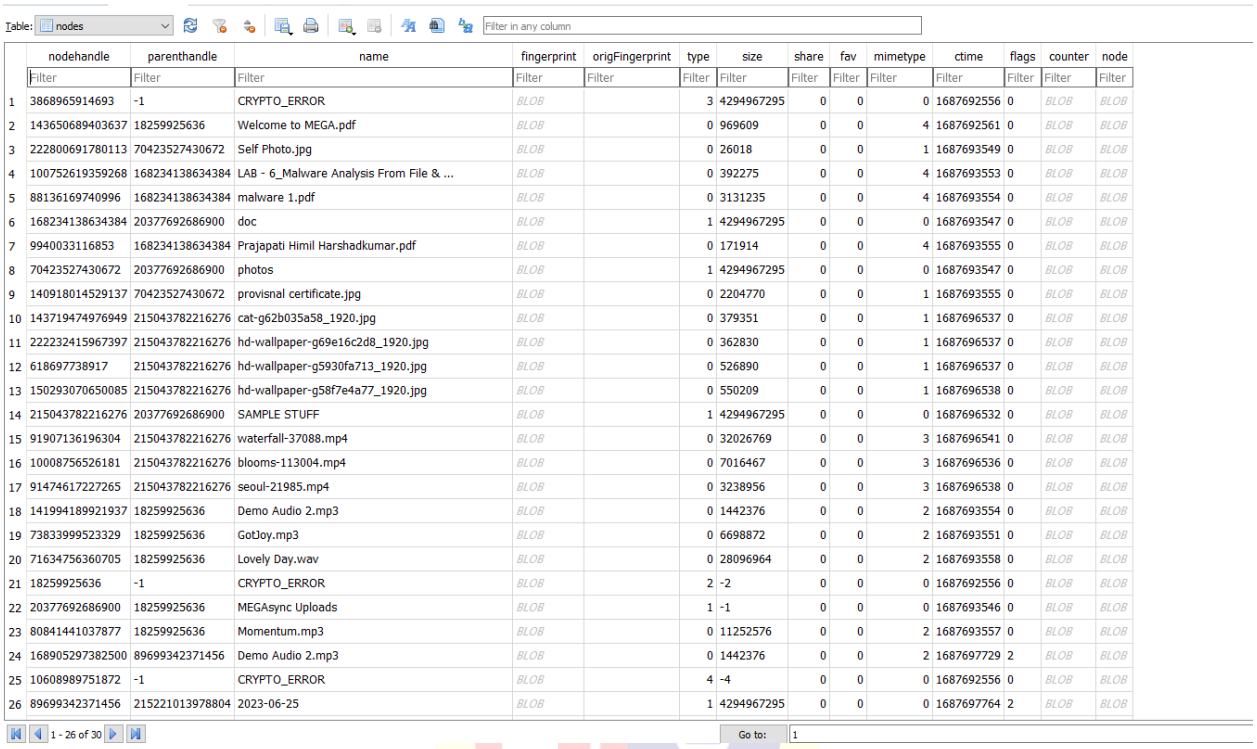


Table: nodes — Filter in any column

	nodehandle	parenthandle	name	fingerprint	origFingerprint	type	size	share	fav	mimetype	ctime	flags	counter	node
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
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	222232415967397	215043782216276	hd-wallpaper-g69e16c2d8_1920.jpg	BLOB		0	362830	0	0	1	1687696537	0	BLOB	BLOB
12	618697738917	215043782216276	hd-wallpaper-g5930fa713_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

1 - 26 of 30 — Go to: 1

Figure 61Sync DB

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

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

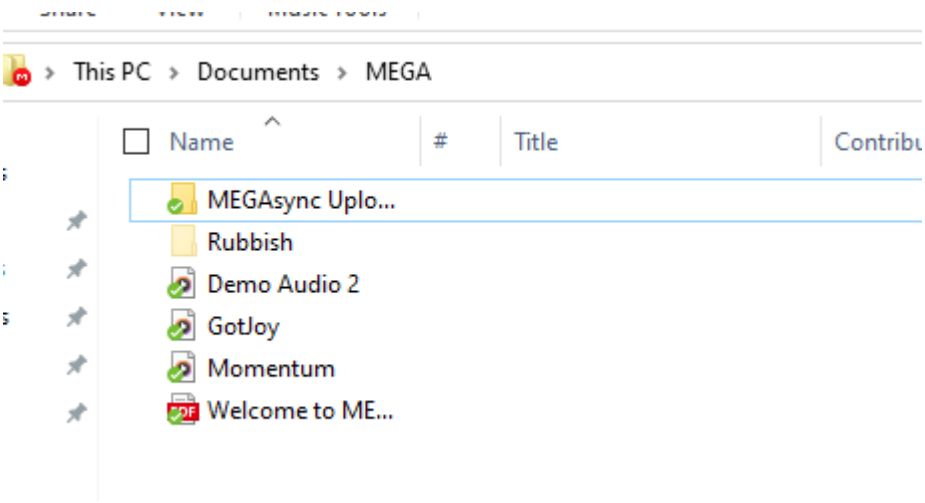


Figure 62List of files are Synced in Cloud

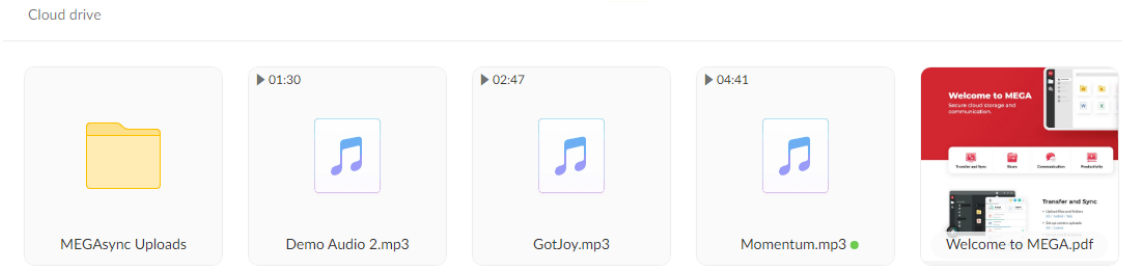


Figure 63Browser view of cloud

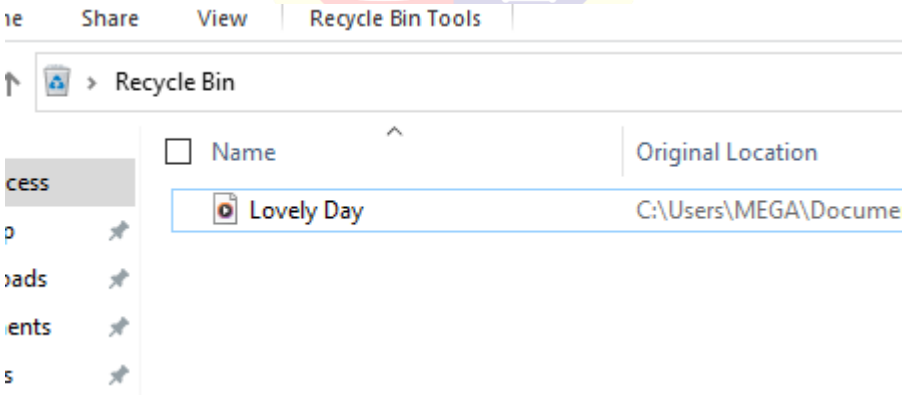


Figure 64Files deleted from cloud effect the PC

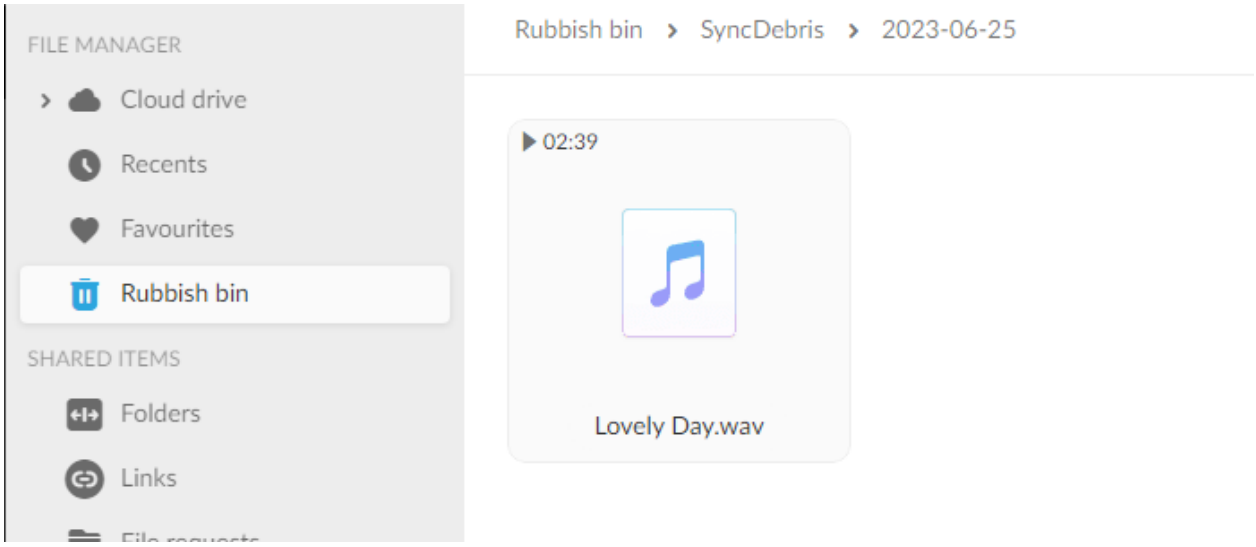


Figure 65 Same effect on browser

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

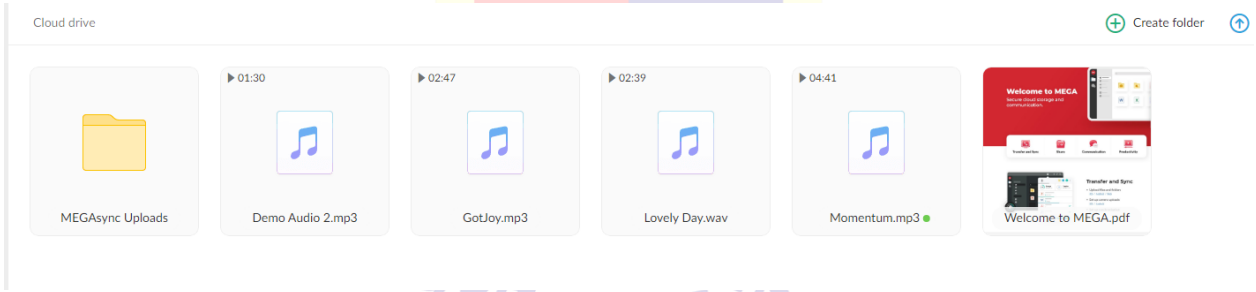


Figure 66 Restore files from the cloud recycle

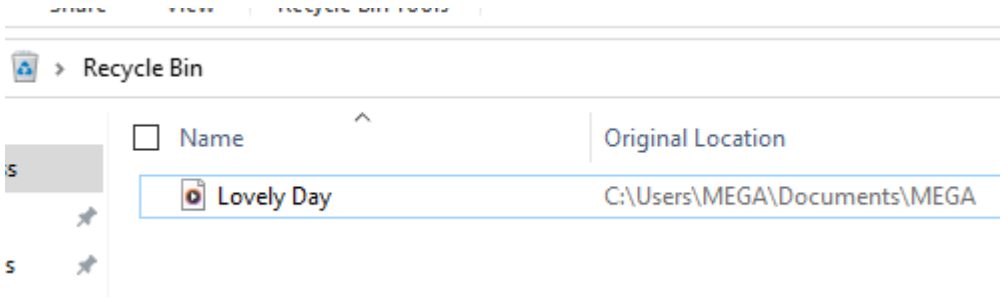


Figure 67 old file in the recycle in PC

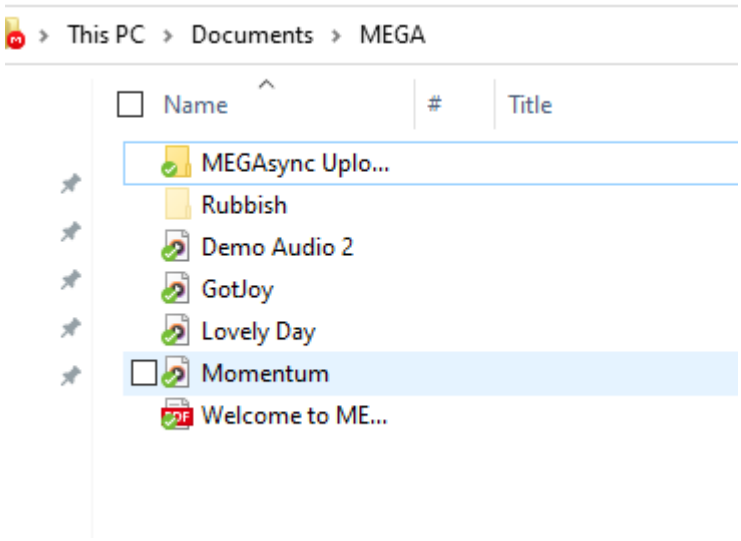


Figure 68New file is created in the Folder

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

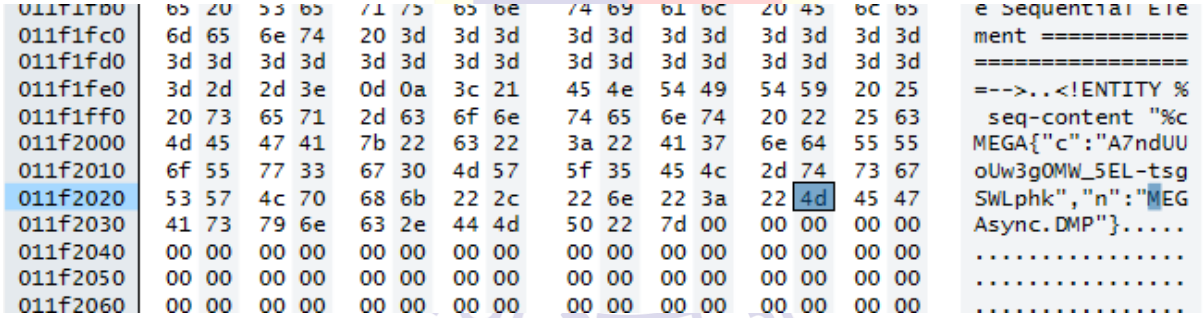


Figure 69Encrypted file sync

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

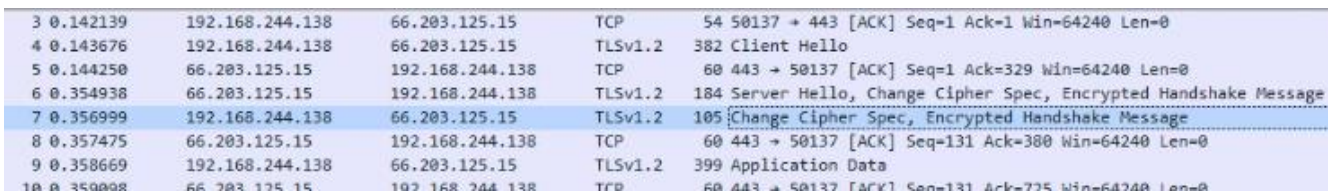


Figure 70Encrypted hand shake

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

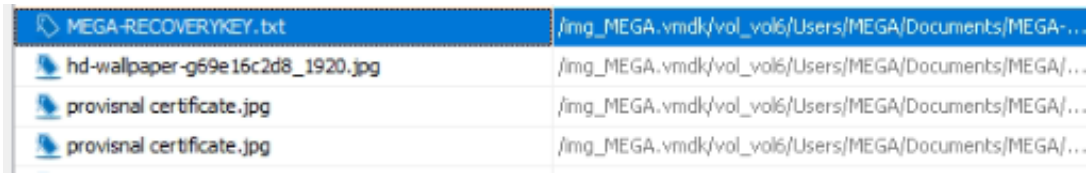


Figure 71Cloud Recovery key

We can find the recover key to recover the cloud

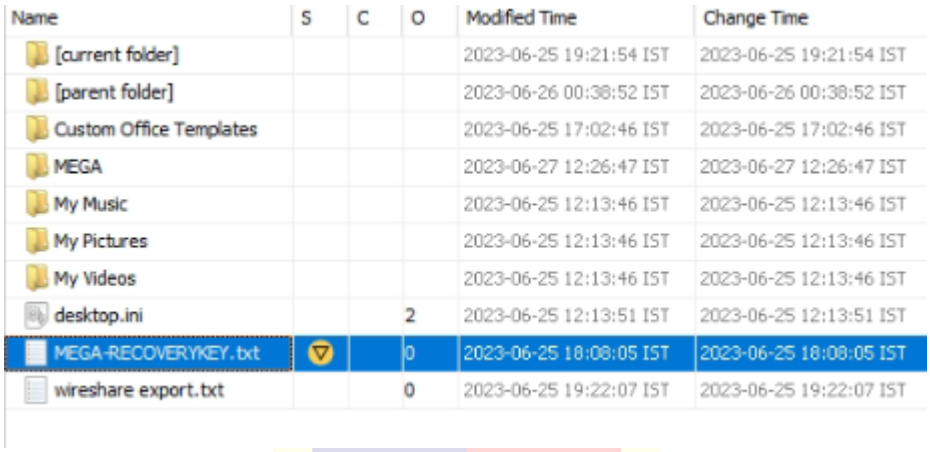


Figure 72Book Mark the key

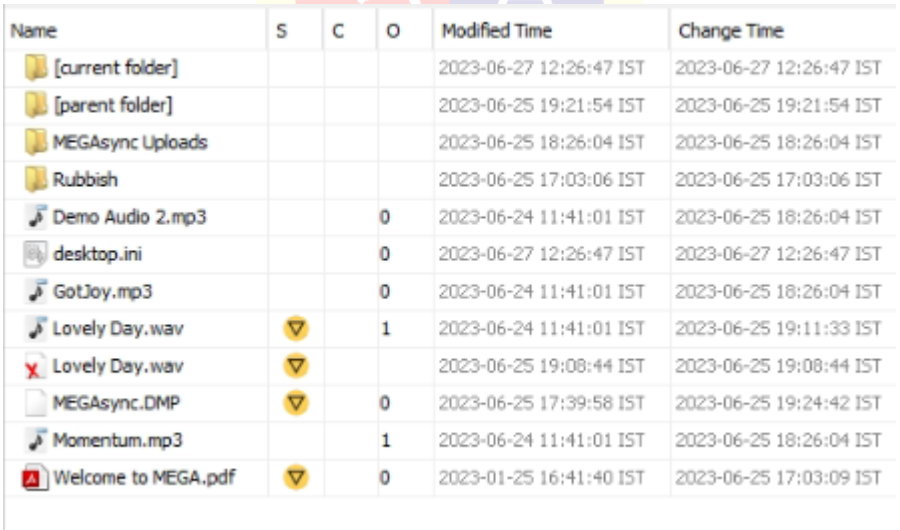


Figure 73Deleted file and sync file list

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

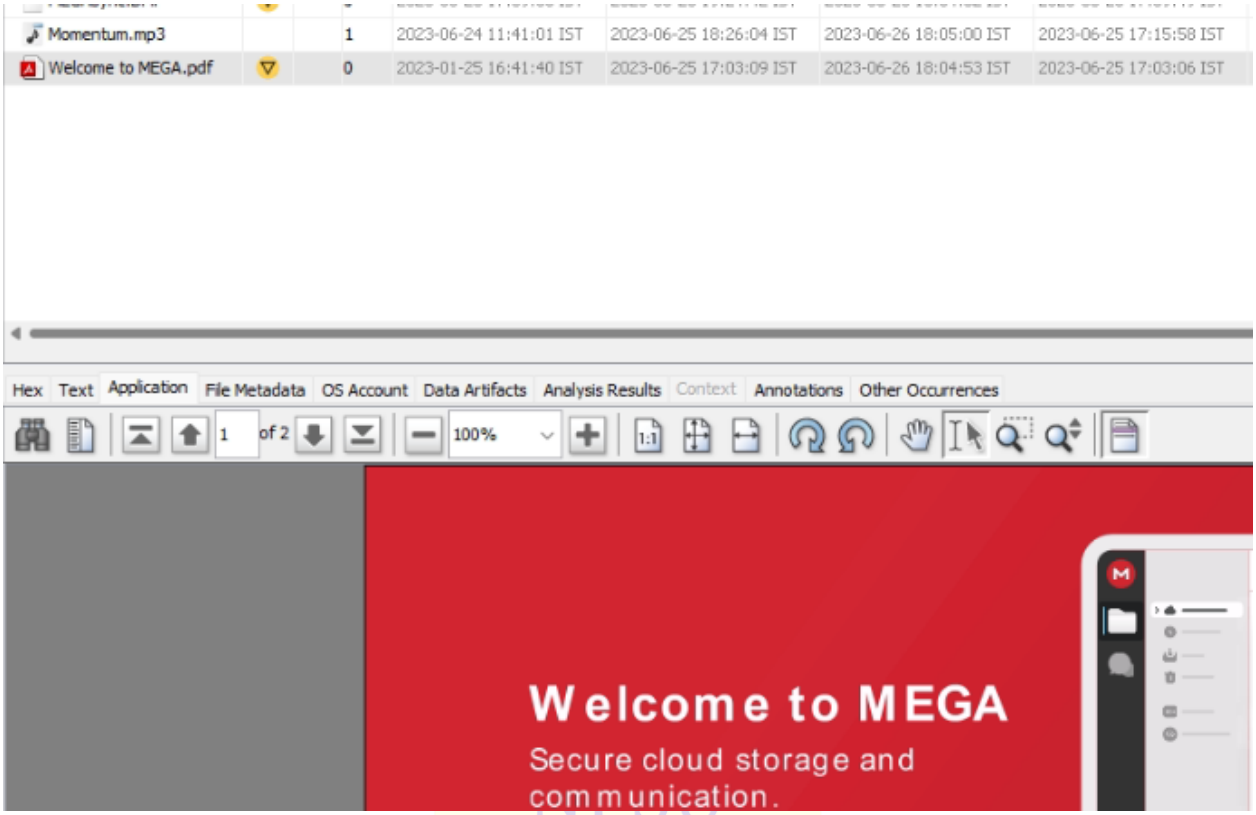


Figure 74Confimed use of the Mega cloud

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

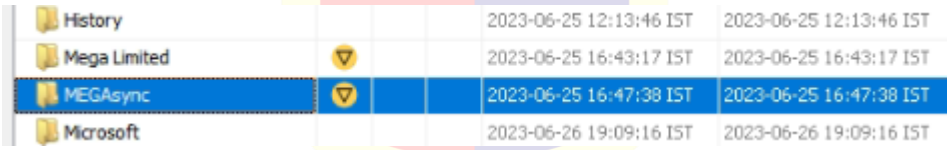


Figure 75Mega sync folder

MegaSyn folder where all the data are store in the cloud

Figure 76Mega version file

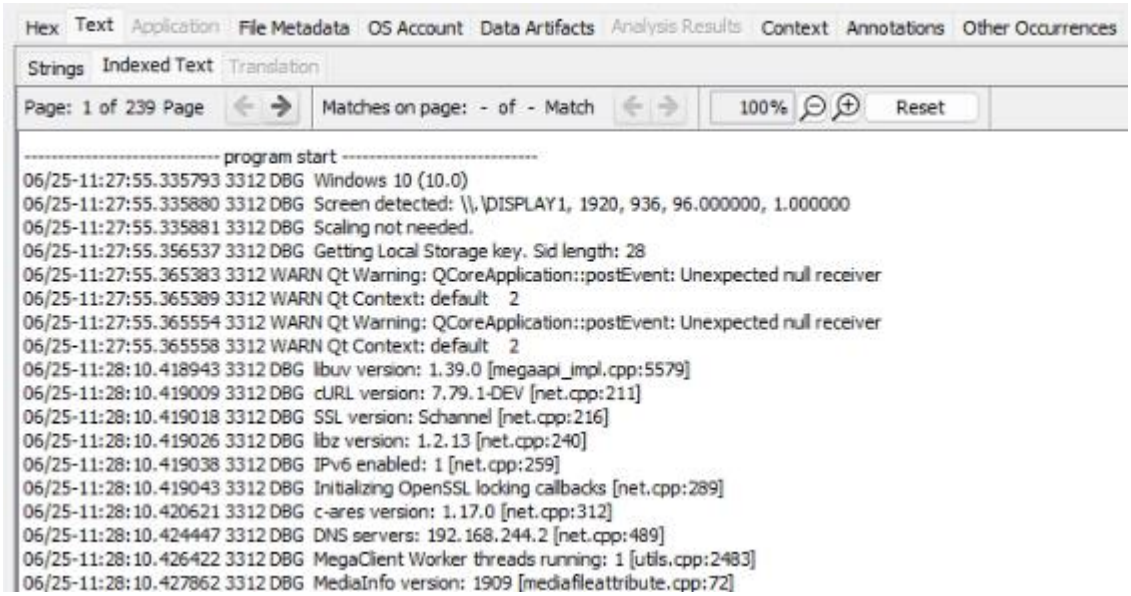


Figure 77Log files

Log files

Figure 78Succesfully installed cloud program

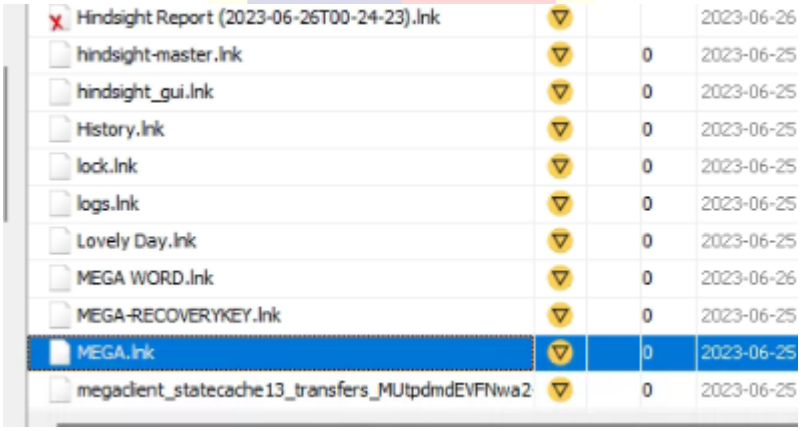


Figure 79all file converted in .lnk which are synced

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

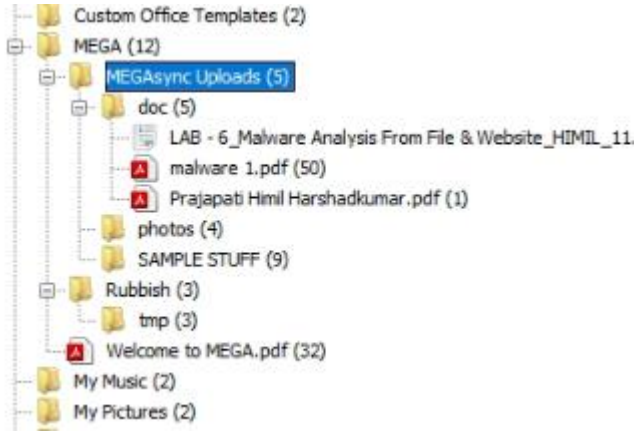


Figure 80synde folder

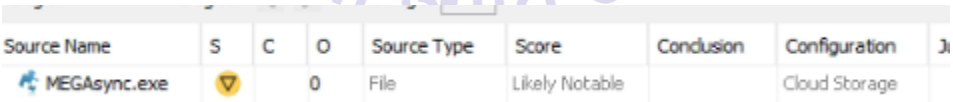
Source Name	S	C	O	Path	Time Deleted	Username	Data Source
$R2CKHSH.wav				C:\Users\MEGA\Documents\MEGA\Lovely Day.wav	2023-06-25 19:08:44 IST		MEGA.vmdk

Figure 81Deleted files

13.4 Browser artifacts

Source Name	S	C	O	Path	URL	D
History			2	C:\Users\MEGA\Downloads\free-hex-editor-neo.exe	https://www.hhdsoftware.com/download/free-hex-editor-...	2
History			2	C:\Users\MEGA\Downloads\Regshot-1.9.0.7z	https://downloads.sourceforge.net/project/regshot/regsh...	2
History			2	C:\Users\MEGA\Downloads\Regshot-1.9.0.7z	https://webwerks.dl.sourceforge.net/project/regshot/regs...	2
History			1	C:\Users\MEGA\Downloads\winrar-x64-622.exe	https://www.win-rar.com/fileadmin/winrar-versions/winrar/...	2
History			1	C:\Users\MEGA\Downloads\Momentum.mp3	blob:https://mega.nz/87b64cc6-aeae-46b4-b0ee-eee1e46...	2
History			1	C:\Users\MEGA\Downloads\MEGAsyncSetup.exe	https://mega.nz/MEGAsyncSetup.exe	2
History				C:\Users\MEGA\Downloads\Hindsight Report (2023-06-26T...	http://localhost:8080/xlsx	2
Regshot-1.9.0.7z:Zone.Identifier			2	/Users/MEGA/Desktop/SAMPLE STUFF/Regshot-1.9.0.7z	https://webwerks.dl.sourceforge.net/project/regshot/regs...	

Figure 82Browser history



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	J
MEGAsync.exe			0	File	Likely Notable		Cloud Storage	

Figure 83Mega cloud .exe

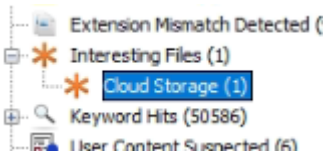
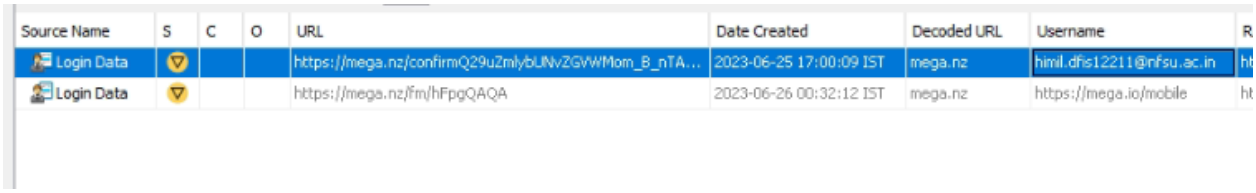
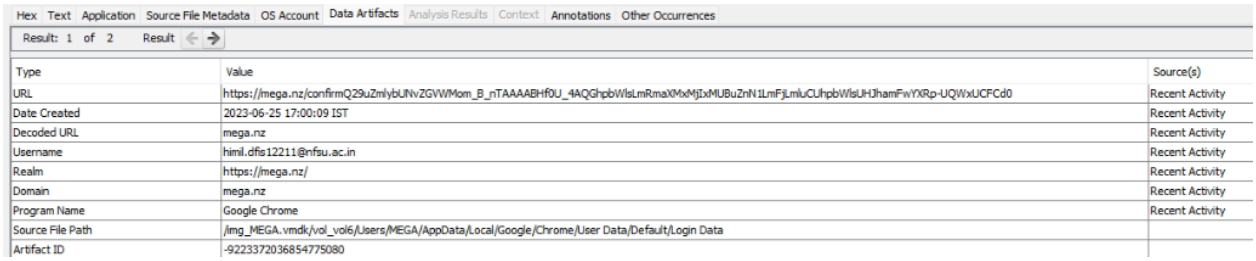


Figure 84Autospy themself create cloud storage separated



Source Name	S	C	O	URL	Date Created	Decoded URL	Username	R
Login Data				https://mega.nz/confirmQ29uZmlybUNvZGVWMom_B_nTA...	2023-06-25 17:00:09 IST	mega.nz	himil.dfis12211@nfsu.ac.in	ht
Login Data				https://mega.nz/fm/hFpgQAQA	2023-06-26 00:32:12 IST	mega.nz	https://mega.io/mobile	ht

Figure 85mega login details

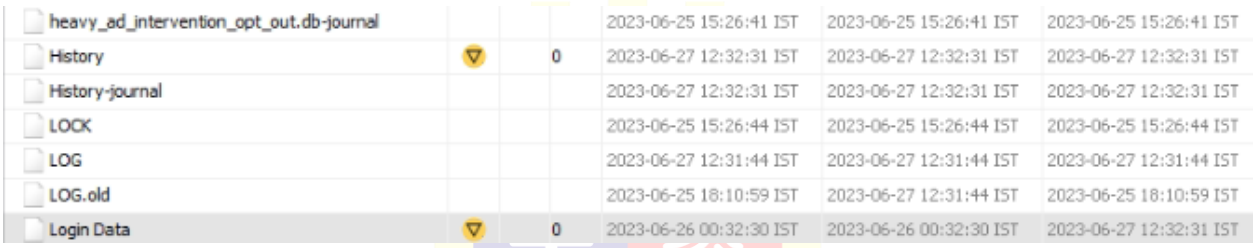


Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 2 Result

Type	Value	Source(s)
URL	https://mega.nz/confirmQ29uZmlybUNvZGVWMom_B_nTAAAABHf0U_4AQGhpbWlsLmRmaXMxMjIxMUBuZnN1LmFjLmluCUhpbWlsUHJhamFwYXRp-UQWxUCFCd0	Recent Activity
Date Created	2023-06-25 17:00:09 IST	Recent Activity
Decoded URL	mega.nz	Recent Activity
Username	himil.dfis12211@nfsu.ac.in	Recent Activity
Realm	https://mega.nz/	Recent Activity
Domain	mega.nz	Recent Activity
Program Name	Google Chrome	Recent Activity
Source File Path	/img_MEGA.vmdk/vol_vol6/Users/MEGA/AppData/Local/Google/Chrome/User Data/Default/Login Data	
Artifact ID	-9223372036854775080	

Figure 86 Recent activity of login mega cloud



heavy_ad_intervention_opt_out.db-journal			2023-06-25 15:26:41 IST	2023-06-25 15:26:41 IST	2023-06-25 15:26:41 IST
History		0	2023-06-27 12:32:31 IST	2023-06-27 12:32:31 IST	2023-06-27 12:32:31 IST
History-journal			2023-06-27 12:32:31 IST	2023-06-27 12:32:31 IST	2023-06-27 12:32:31 IST
LOCK			2023-06-25 15:26:44 IST	2023-06-25 15:26:44 IST	2023-06-25 15:26:44 IST
LOG			2023-06-27 12:31:44 IST	2023-06-27 12:31:44 IST	2023-06-27 12:31:44 IST
LOG.old			2023-06-25 18:10:59 IST	2023-06-27 12:31:44 IST	2023-06-25 18:10:59 IST
Login Data		0	2023-06-26 00:32:30 IST	2023-06-26 00:32:30 IST	2023-06-27 12:32:31 IST

Figure 87Login DATA files

Login data history

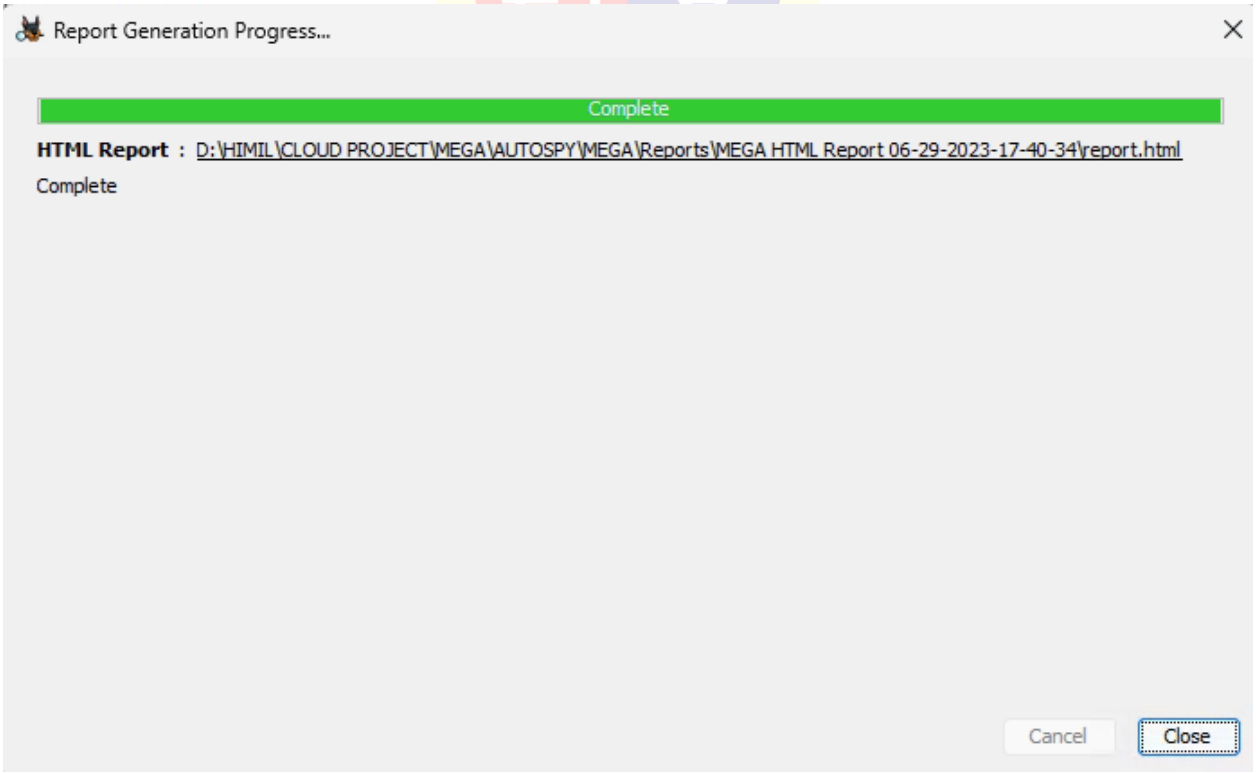


Figure 88 Report make from autopsy successfully

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

A	B	C	D	E
Hindsight Internet History Forensics (v2023.03)				
Type	Timestamp (US/Pacif	URL	Title / Name / Status	Data / Value / Path
preference (sessio	2023-06-25 02:56:37.036		Session event log [in Prefere	{'crashed': False, 'time': '13332160597036707', 'type': 0}
preference (sessio	2023-06-25 03:50:46.829		Session event log [in Prefere	{'did_schedule_command': True, 'first_session_service': Tr
preference (sessio	2023-06-25 03:57:06.415		Session event log [in Prefere	{'crashed': False, 'time': '13332164226415565', 'type': 0}
url	2023-06-25 03:57:38.522	https://www.google.com/search?q=hexeditor&oq=hexeditor&gs_lc	hexeditor - Google Search	
url	2023-06-25 03:57:39.232	https://www.google.com/search?q=hexeditor&oq=hexeditor&gs_lc	hexeditor - Google Search	
url	2023-06-25 03:57:43.814	https://www.hhdsoftware.com/free-hex-editor	Free Hex Editor: Fastest Binary File Editing Software. Freeware. Windows	
download	2023-06-25 03:57:49.109	https://www.hhdsoftware.com/download/free-hex-editor-neo.exe	Complete - 100% [22117632/	C:\Users\MEGA\Downloads\free-hex-editor-neo.exe
url	2023-06-25 04:04:26.387	https://www.google.com/search?q=gmail&oq=gmail&gs_lcrp=EgZjal	gmail - Google Search	
url	2023-06-25 04:04:27.060	https://www.google.com/search?q=gmail&oq=gmail&gs_lcrp=EgZjal	gmail - Google Search	
url	2023-06-25 04:04:30.098	https://mail.google.com/?	Inbox - himil.dfis12211@nfsu.ac.in - National Forensic Sciences University Mail	
url	2023-06-25 04:04:30.098	https://mail.google.com/mail/	Inbox - himil.dfis12211@nfsu.ac.in - National Forensic Sciences University Mail	
url	2023-06-25 04:04:30.098	https://mail.google.com/mail/u/0/	Inbox - himil.dfis12211@nfsu.ac.in - National Forensic Sciences University Mail	
url	2023-06-25 04:04:30.098	https://accounts.google.com/ServiceLogin?service=mail&passive=12	Gmail: Private and secure email at no cost | Google Workspace	
url	2023-06-25 04:04:30.098	https://mail.google.com/intl/en-US/mail/help/about.html	Gmail: Private and secure email at no cost | Google Workspace	
url	2023-06-25 04:04:30.098	https://www.google.com/intl/en-US/mail/help/about.html	Gmail: Private and secure email at no cost | Google Workspace	
url	2023-06-25 04:04:30.098	https://www.google.com/gmail/about/	Gmail: Private and secure email at no cost | Google Workspace	
url	2023-06-25 04:04:32.593	https://accounts.google.com/AccountChooser/signinchooser?servic	Gmail	
url	2023-06-25 04:04:32.593	https://accounts.google.com/AccountChooser?service=mail&contin	Gmail	
url	2023-06-25 04:04:32.593	https://accounts.google.com/ServiceLogin?continue=https%3A%2F9	Gmail	
url	2023-06-25 04:04:32.593	https://accounts.google.com/InteractiveLogin?continue=https://ma	Gmail	
url	2023-06-25 04:04:32.593	https://accounts.google.com/v3/signin/identifier?dsh=S839065344%	Gmail	
url	2023-06-25 04:04:32.963	https://accounts.google.com/v3/signin/identifier?dsh=S839065344%	Gmail	
site setting (modif	2023-06-25 04:05:09.415	https://accounts.google.com:443,*	formfill_metadata [in Prefer	{'last_modified': '13332164709415588', 'setting': {'UserDatal
autofill	2023-06-25 04:05:10.000		identifier	himil.dfis12211@nfsu.ac.in
url	2023-06-25 04:05:10.070	https://accounts.google.com/v3/signin/challenge/pwd?TL=AG7eRGE	Gmail	

Figure 89hindsight browser history by timeline

	C:\Users\MEG	Local	0:00:02.497972	1	0	0	link; Nav
| flowName	C:\Users\MEG	Local	None	1	0	0	link; Nav
| flowName	C:\Users\MEG	Local	None	1	0	0	link; Ser
| sacu: 1 | ri	C:\Users\MEG	Local	None	1	0	0	link; Ser
1 | service: n	C:\Users\MEG	Local	None	1	0	0	link; Ser
nail.google.c	C:\Users\MEG	Local	0:00:00.370455	2	0	0	link; Nav
nail.google.c	C:\Users\MEG	Local	0:00:37.110512	2	0	0	link; Nav
	C:\Users\MEGA\AppData\Local\Google\Chrome\User Data\Default						
	C:\Users\MEGA\AppData\Local\Google\Chrome\User Data\Default						
PSghgvlql-74	C:\Users\MEG	Local	0:00:18.961433	1	0	0	link; Nav
	C:\Users\MEGA\AppData\Local\Google\Chrome\User Data\Default						
	C:\Users\MEGA\AppData\Local\Google\Chrome\User Data\Default						
	C:\Users\MEGA\AppData\Local\Google\Chrome\User Data\Default						

Figure 90hindsight browser history find

14. One drive

14.1 installation process

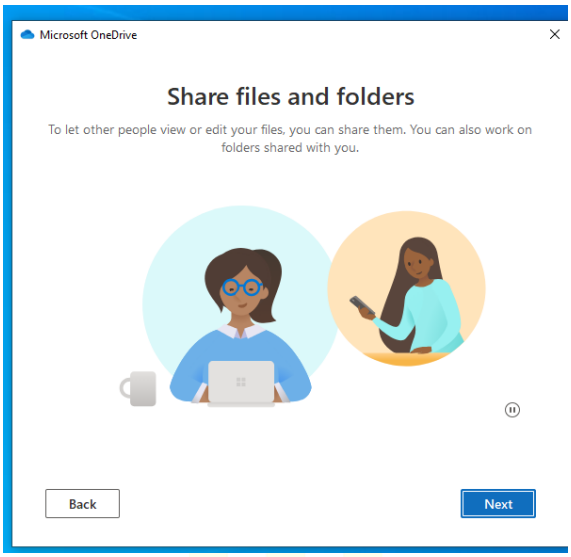


Figure 91installtion steps

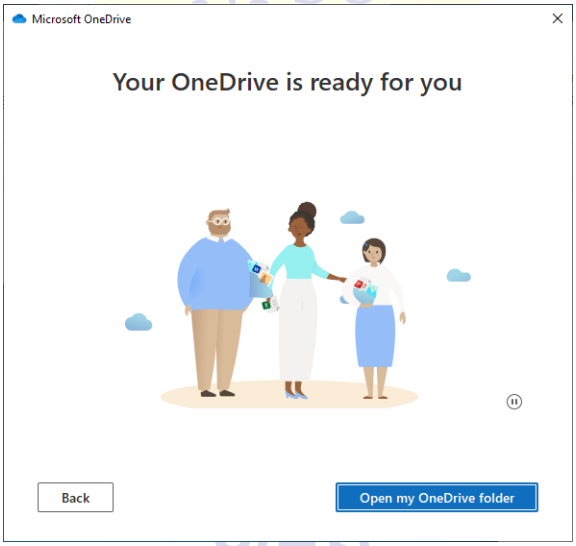


Figure 92successfully installed

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

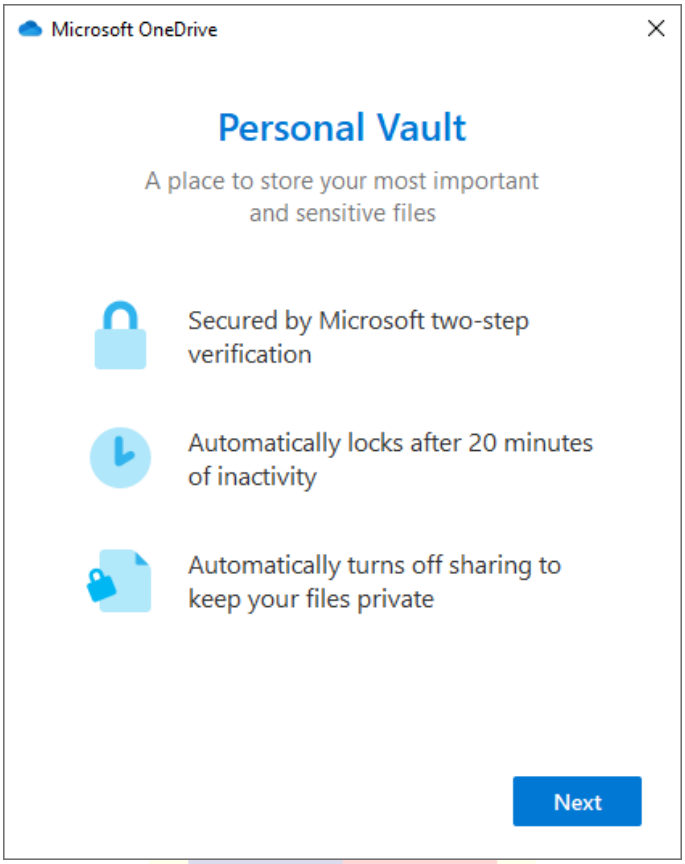
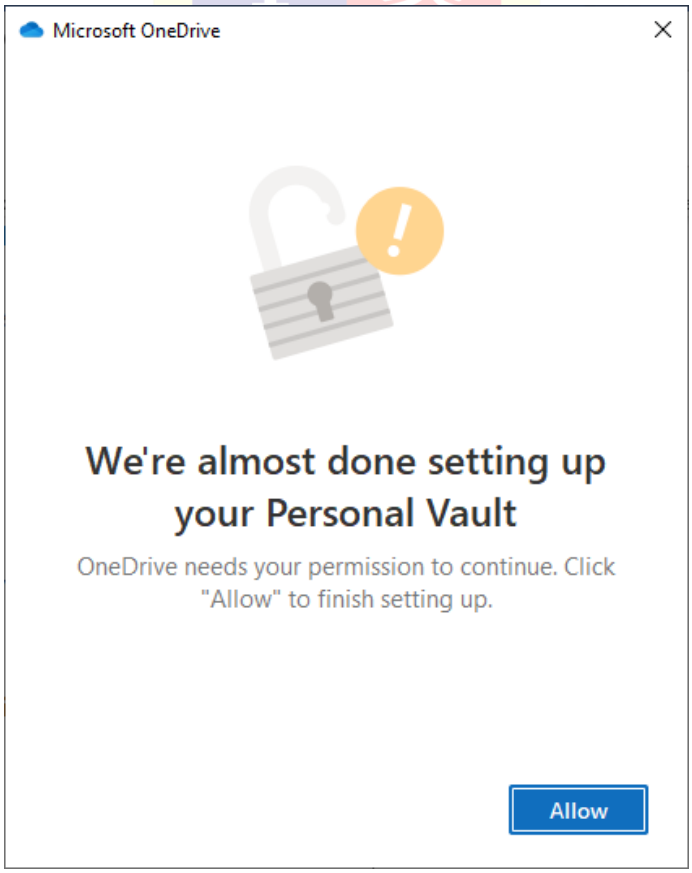


Figure 93Pernal vault setup



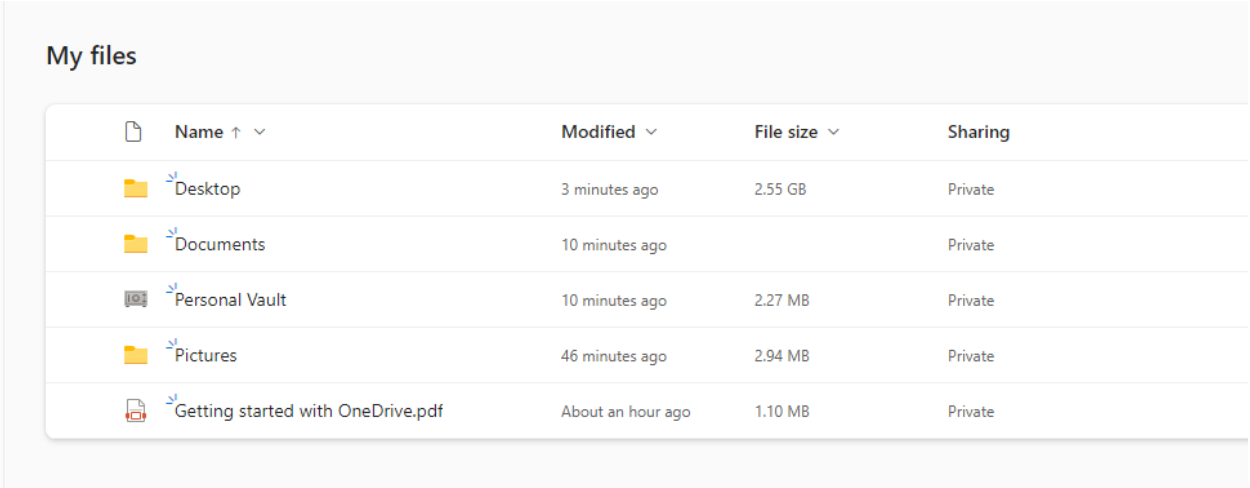


Figure 94Sync folder list

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

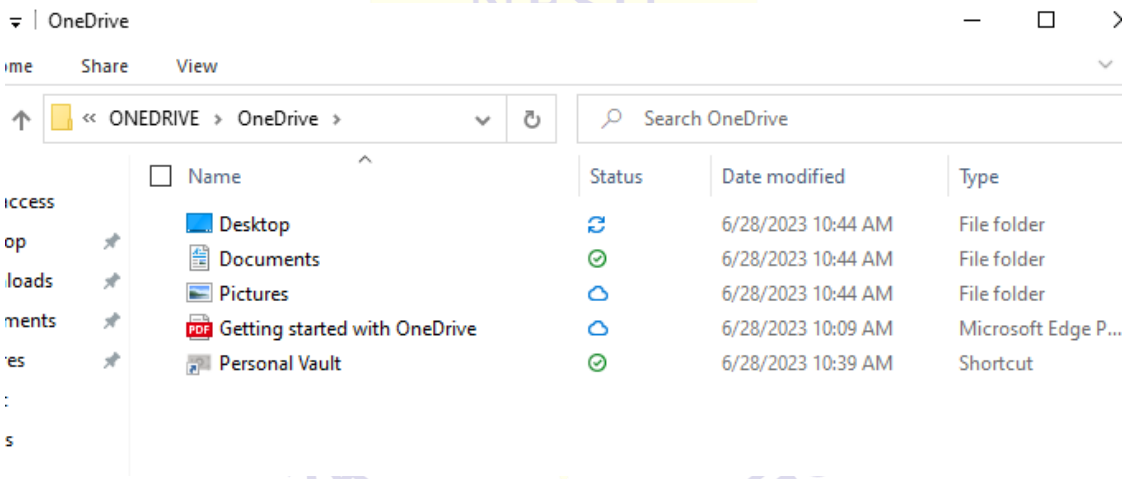


Figure 95sync status

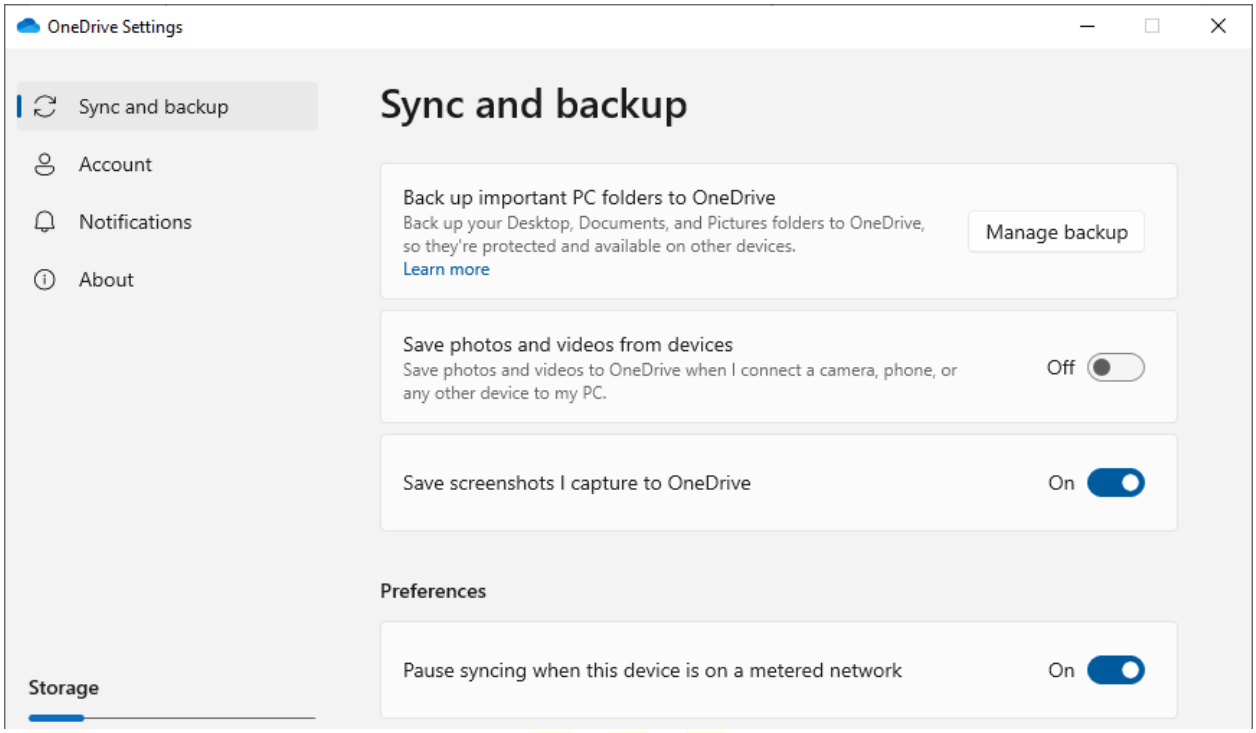


Figure 96Sync and backup folder setting

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

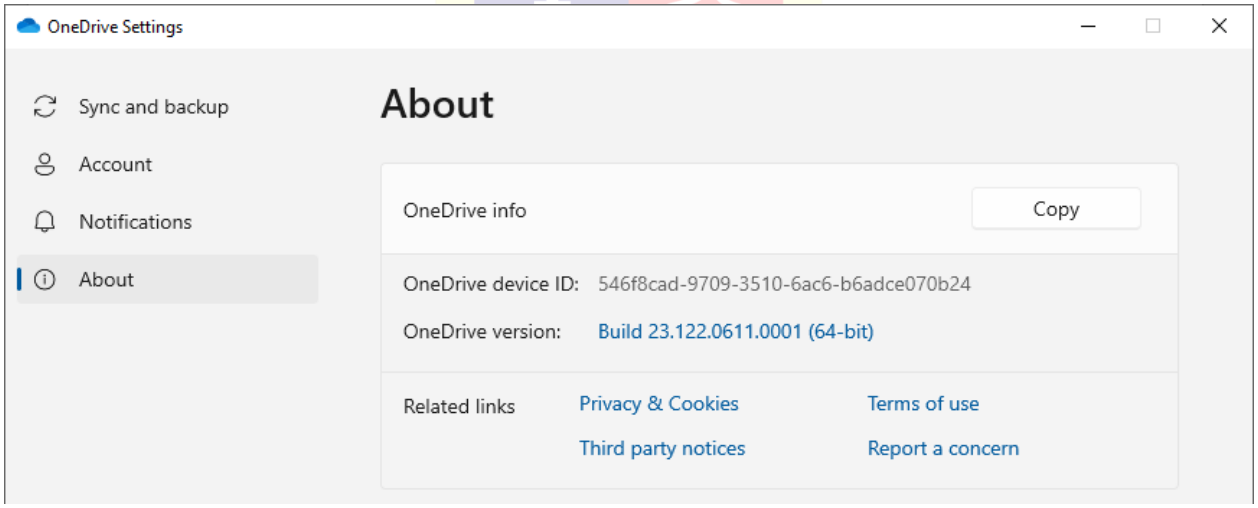


Figure 97 Version of the one drive

Version of the one drive device id of the

14.2 RAM Dump

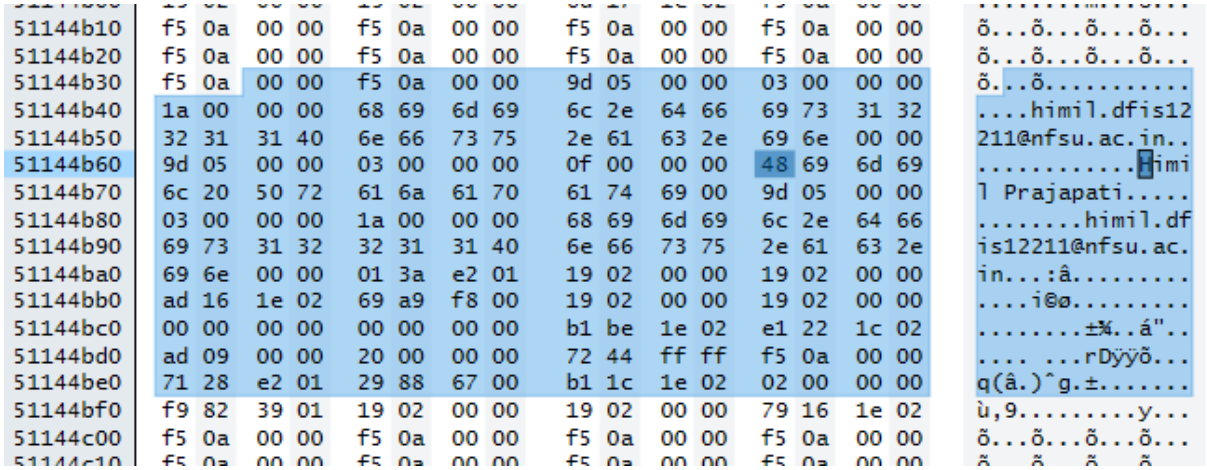


Figure 98User id Reveal Ram Dump

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

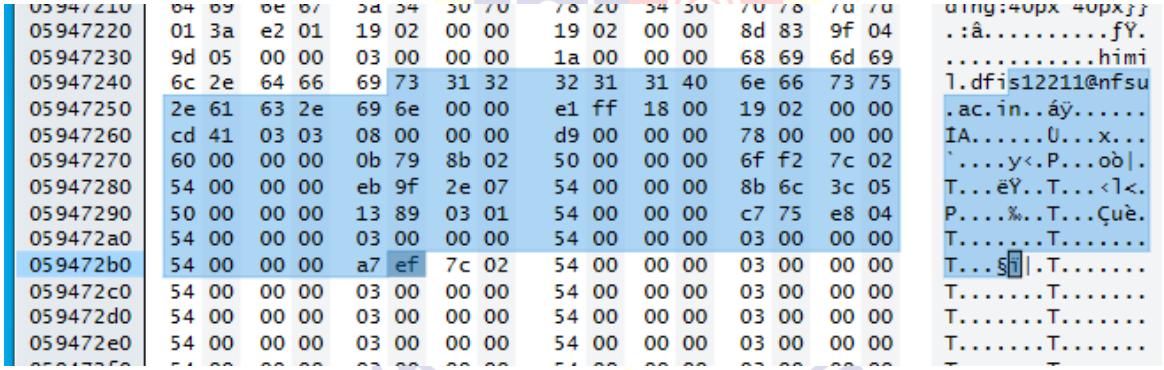


Figure 99Encypted password

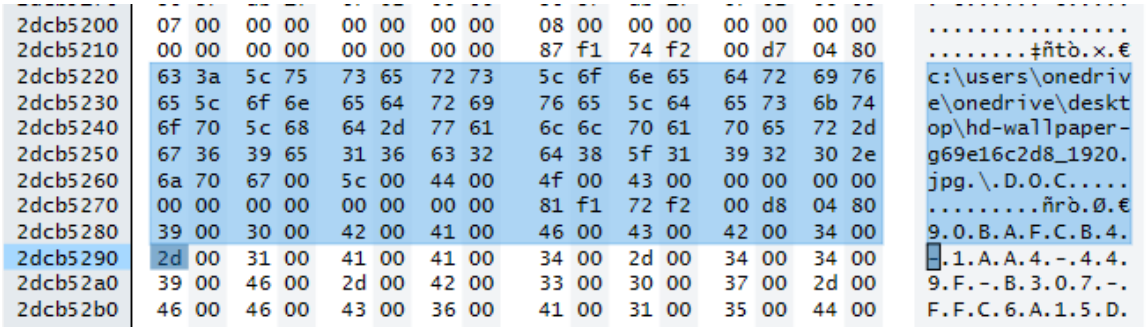


Figure 100Sync File Location reveal in ram dump

Setup log file in the plain text

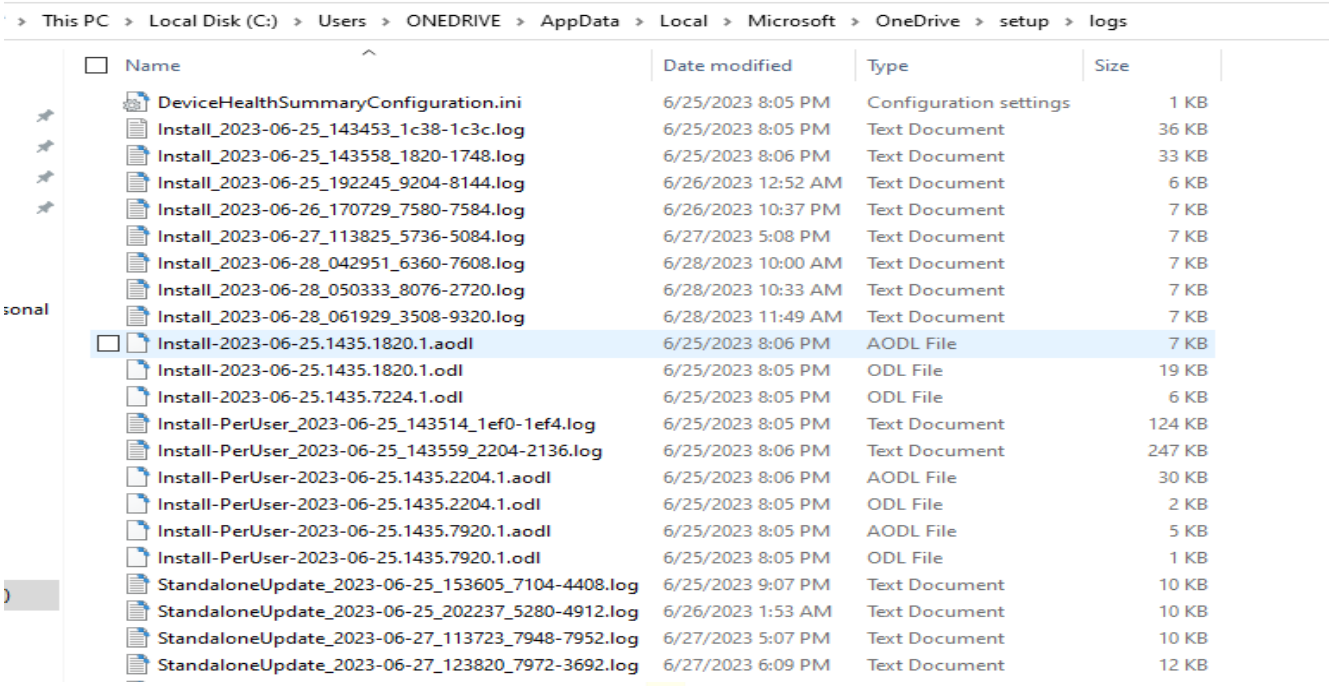


Figure 101Log Files

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 syncdiagnistics.log file

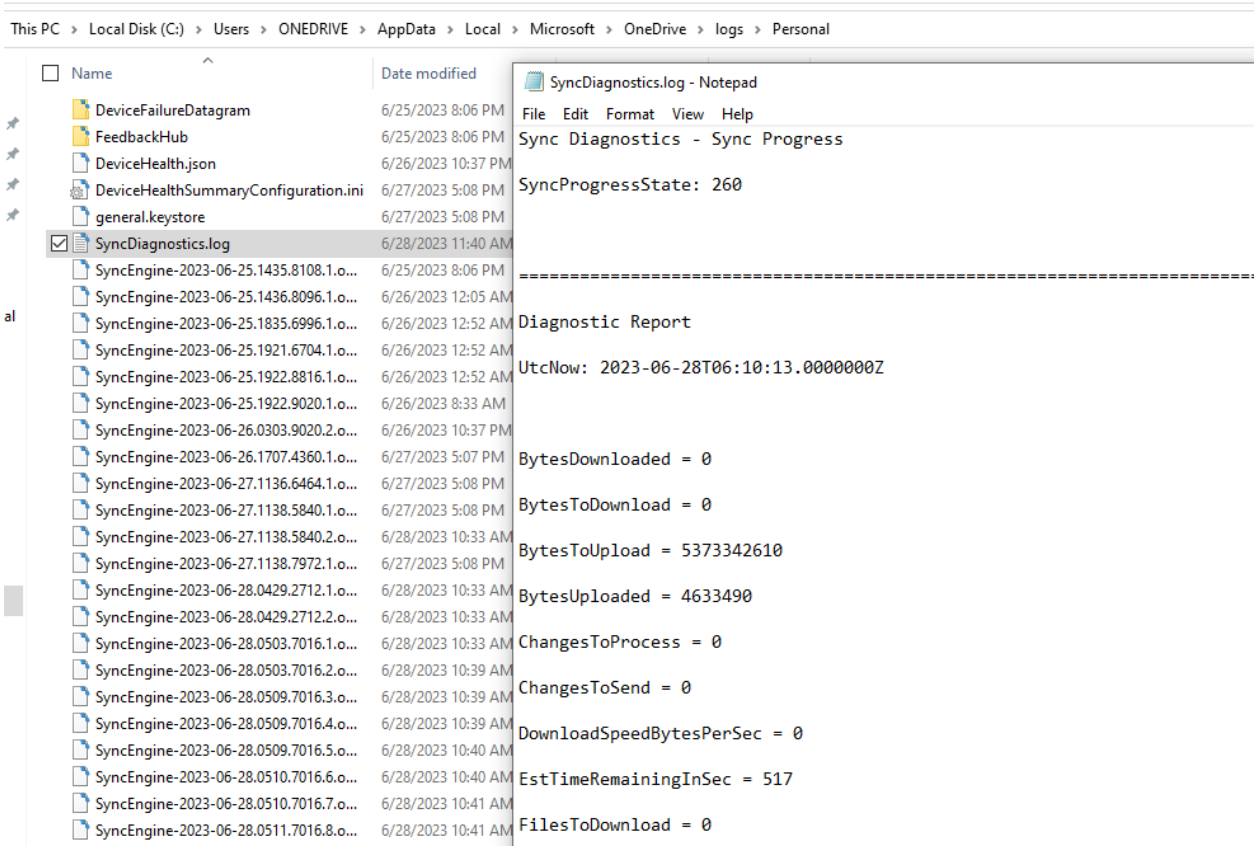


Figure 102SyncDiagnostics.log for track all thinks

One drive also the hold the info of the device also in plain text with the version and the last report time in plain text

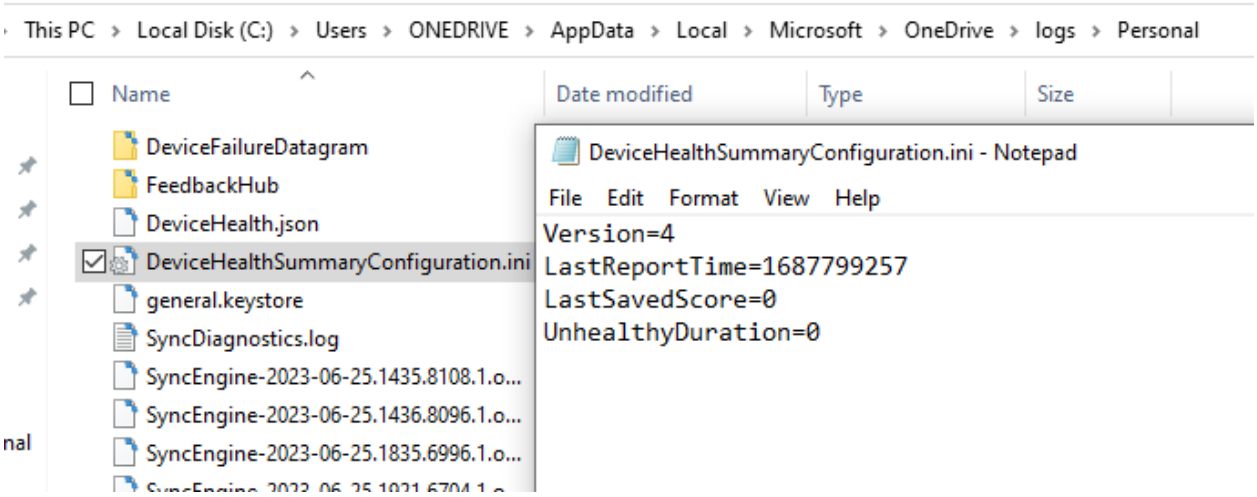


Figure 103Device health summary track

14.3 Disk creation

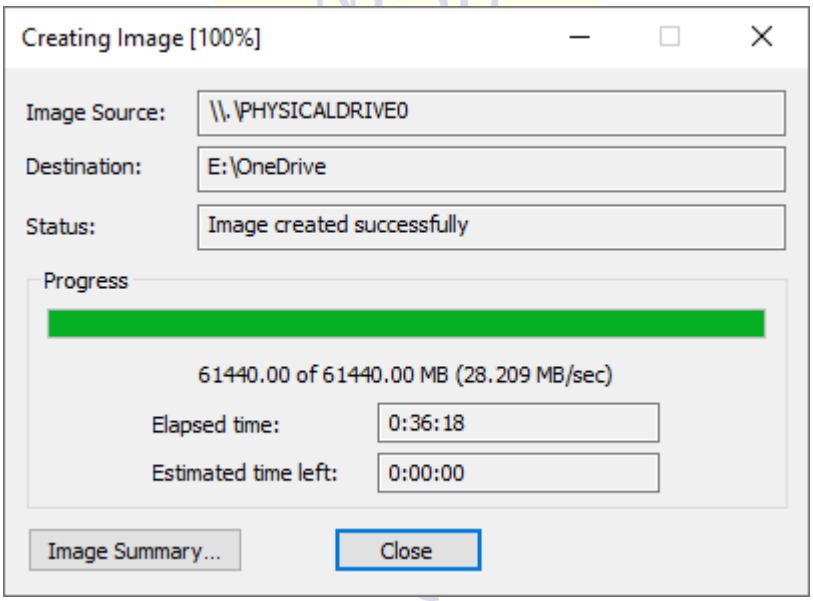


Figure 104image creation

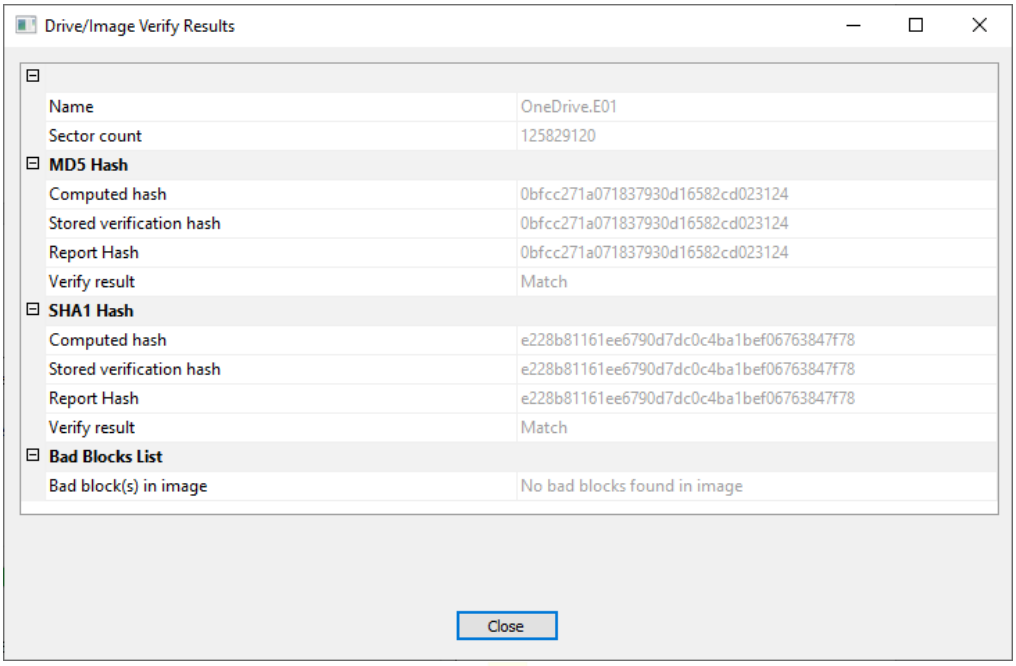


Figure 105successfully created image

14.4 One drive disk analysis

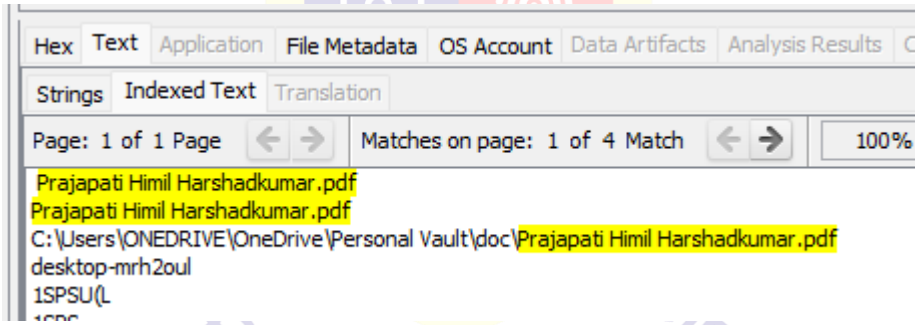


Figure 106 Vault location

We can find the trace of the location even I can find the file as the pdf extracted that from the autopsy after also we cannot the open the pdf file or we cannot edit the state of the pdf from the setting also

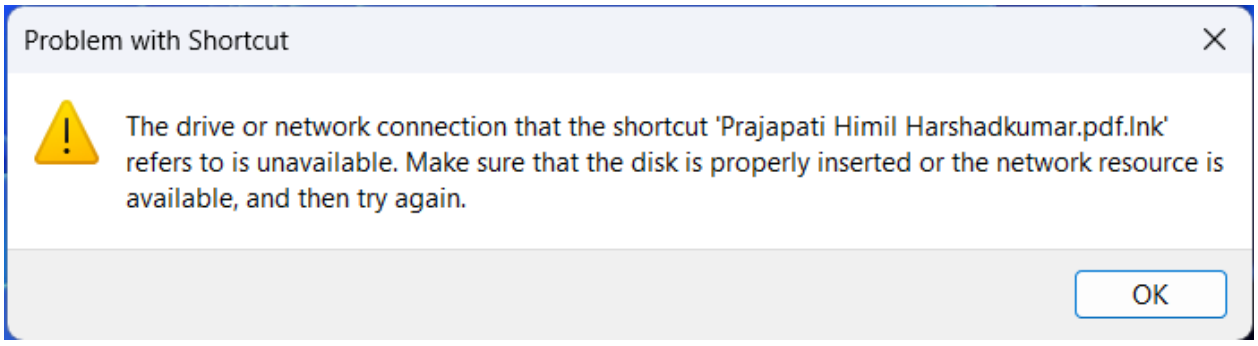


Figure 107all files are in .lnk which are not open

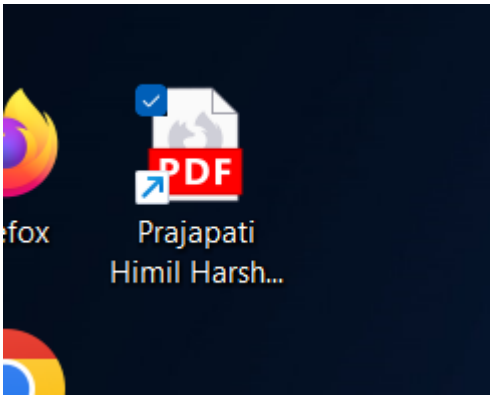


Figure 108.lnk files recovered

LOCK.lnk	C:\Users\ONEDRIVE\AppData\Local\Microsoft\OneDrive\EB...	0000-00-00 00:00:00 OneDrive.E01
LOG.lnk	C:\Users\ONEDRIVE\AppData\Local\Microsoft\OneDrive\EB...	0000-00-00 00:00:00 OneDrive.E01
CURRENT.lnk	C:\Users\ONEDRIVE\AppData\Local\Microsoft\OneDrive\EB...	0000-00-00 00:00:00 OneDrive.E01
DeviceHealthSummaryConfiguration.ini.lnk	C:\Users\ONEDRIVE\AppData\Local\Microsoft\OneDrive\lo...	0000-00-00 00:00:00 OneDrive.E01
Screenshot (5).png.lnk	C:\Users\ONEDRIVE\OneDrive\Pictures\Screenshots\Scree...	0000-00-00 00:00:00 OneDrive.E01
provisnal certificate.jpg.lnk	C:\Users\ONEDRIVE\OneDrive\Personal Vault\doc\provisna...	0000-00-00 00:00:00 OneDrive.E01
Prajapati Himil Harshadkumar.pdf.lnk	C:\Users\ONEDRIVE\OneDrive\Personal Vault\doc\Prajapat...	0000-00-00 00:00:00 OneDrive.E01
Screenshot (1).png.lnk	C:\Users\ONEDRIVE\OneDrive\Pictures\Screenshots\Scree...	0000-00-00 00:00:00 OneDrive.E01

Figure 109all files in .lnk

In the future of the recent documents also we can find the use of the vault document but we cannot extract the files but we got the lead for the case that the use of the vault of the one drive to safe the document we got the location also.

Result: 1 of 1 Result

Type	Value	Source(s)
Path	C:\Users\ONEDRIVE\OneDrive\Personal Vault\doc\provisnal certificate.jpg	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	0000-00-00 00:00:00	RecentActivity
Source File Path	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/5f7b5f1e01b83767.automaticDestinations-ms/provisnal certificate.jpg.lnk	
Artifact ID	-9223372036854775642	

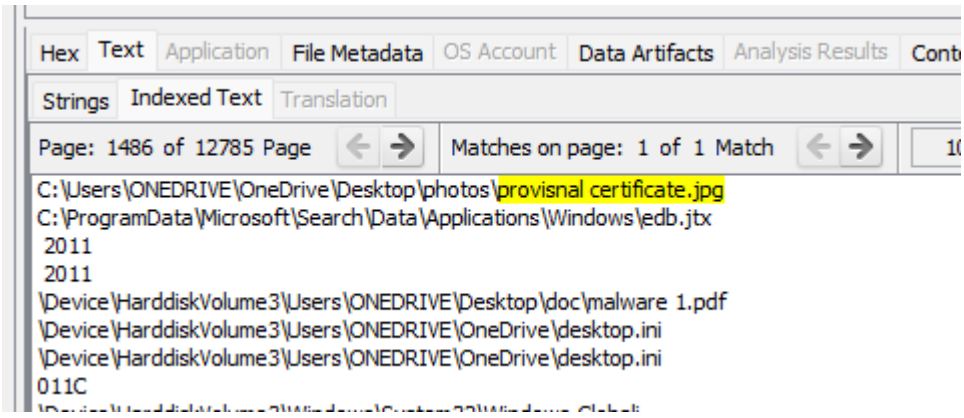


Figure 110 fist location of file found and recover

The file first store in the desktop and after that the user is tore that file in the personal vault

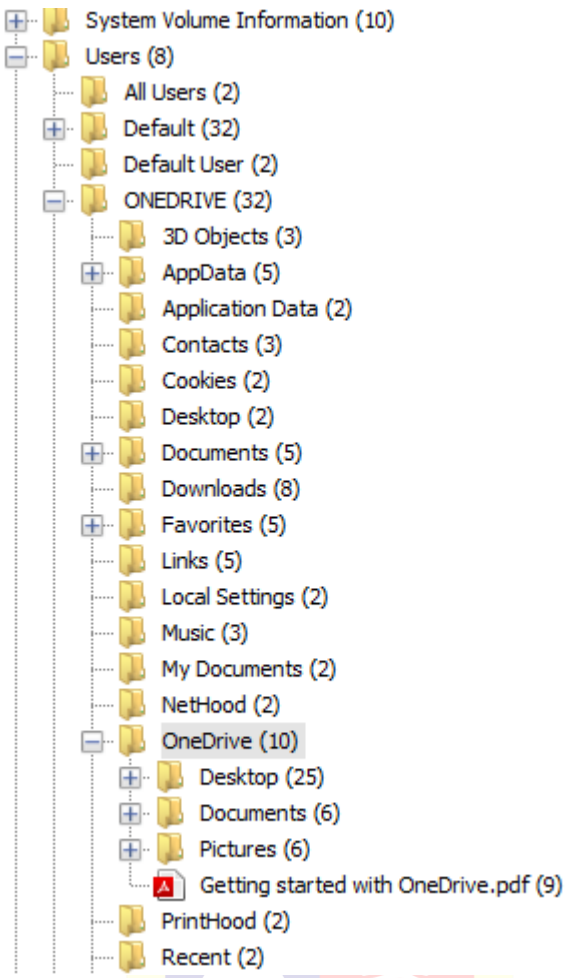


Figure 111Desktop empty all files in cloud

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 one drive

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2023-06-28 11:57:59 IST	2023-06-28 11:57:59 IST	2023-06-28 17:07:03 IST	2023-06-25 20:05:36 IST
[parent folder]				2023-06-28 10:41:00 IST	2023-06-28 10:41:00 IST	2023-06-28 17:42:21 IST	2023-06-25 20:03:17 IST
Desktop				2023-06-28 13:46:57 IST	2023-06-28 13:46:57 IST	2023-06-28 17:07:03 IST	2023-06-28 10:40:55 IST
Documents				2023-06-28 13:46:56 IST	2023-06-28 13:46:56 IST	2023-06-28 17:32:09 IST	2023-06-28 10:39:53 IST
Pictures				2023-06-28 13:46:57 IST	2023-06-28 13:46:57 IST	2023-06-28 17:30:42 IST	2023-06-28 10:39:53 IST
.849C9593-D756-4E56-8D6E-42412F2A707B			0	2023-06-28 10:39:52 IST	2023-06-28 10:39:55 IST	2023-06-28 10:39:52 IST	2023-06-28 10:39:52 IST
desktop.ini			2	2023-06-26 00:47:15 IST	2023-06-28 10:39:54 IST	2023-06-28 17:07:03 IST	2023-06-25 20:05:36 IST
Getting started with OneDrive.pdf			0	2023-06-28 10:09:35 IST	2023-06-28 17:56:10 IST	2023-06-28 17:56:10 IST	2023-06-28 10:39:53 IST
Personal Vault.lnk			0	2023-06-28 11:57:59 IST	2023-06-28 17:29:21 IST	2023-06-28 17:29:21 IST	2023-06-28 10:39:53 IST
Personal Vault.lnk:${3D0CE612-FDEE-43f7-8ACA-957BE			0	2023-06-28 11:57:59 IST	2023-06-28 17:29:21 IST	2023-06-28 17:29:21 IST	2023-06-28 10:39:53 IST

Figure 112list 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

1. Desktop we can find all the files are user and deleted from the desktop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
photos				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ProcessMonitor				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Regshot-1.9.0				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
SAMPLE STUFF				2023-06-28 10:40:57 IST	2023-06-28 10:41:05 IST	2023-06-28 17:28:31 IST	2023-06-28 10:40:55 IST
blooms-113004.mp4			1	2023-04-25 16:39:34 IST	2023-06-28 17:32:09 IST	2023-06-28 17:32:09 IST	2023-05-05 11:48:41 IST
cat-g62b035a58_1920.jpg			1	2023-04-25 16:37:36 IST	2023-06-28 17:32:12 IST	2023-06-28 17:32:12 IST	2023-05-05 11:48:41 IST
desktop.ini			1	2023-06-28 13:46:57 IST	2023-06-28 13:47:00 IST	2023-06-28 17:07:03 IST	2023-06-25 20:03:22 IST
hd-wallpaper-g58f7e4a77_1920.jpg			1	2023-04-25 16:38:43 IST	2023-06-28 17:32:12 IST	2023-06-28 17:32:12 IST	2023-05-05 11:48:41 IST
hd-wallpaper-g5930fa713_1920.jpg			1	2023-04-25 16:39:16 IST	2023-06-28 17:32:12 IST	2023-06-28 17:32:12 IST	2023-05-05 11:48:41 IST
hd-wallpaper-g69e16c2d8_1920.jpg			1	2023-04-25 16:38:02 IST	2023-06-28 17:32:13 IST	2023-06-28 17:32:13 IST	2023-05-05 11:48:41 IST
Hex Editor Neo.lnk			0	2023-06-26 00:38:31 IST	2023-06-28 17:28:26 IST	2023-06-28 17:28:26 IST	2023-06-26 00:38:31 IST
hindsight.log			0	2023-06-28 13:42:35 IST	2023-06-28 17:32:13 IST	2023-06-28 17:32:13 IST	2023-06-28 11:52:10 IST
hindsight_gui - Shortcut.lnk			0	2023-06-26 00:49:08 IST	2023-06-28 17:28:26 IST	2023-06-28 17:28:26 IST	2023-06-26 00:49:08 IST
memdump.mem			0	2023-06-28 10:45:40 IST	2023-06-28 17:32:13 IST	2023-06-28 17:32:13 IST	2023-06-28 10:45:17 IST
memdump.mem:${3D0CE612-FDEE-43f7-8ACA-957BEC			0	2023-06-28 10:45:40 IST	2023-06-28 17:32:13 IST	2023-06-28 17:32:13 IST	2023-06-28 10:45:17 IST
Microsoft Edge.lnk			0	2023-06-26 00:38:42 IST	2023-06-28 17:28:26 IST	2023-06-28 17:28:26 IST	2023-06-25 20:03:22 IST
Microsoft Teams.lnk			0	2023-06-26 01:17:43 IST	2023-06-28 17:28:26 IST	2023-06-28 17:28:26 IST	2023-06-26 00:52:12 IST
One drive.docx			0	2023-06-28 12:22:01 IST	2023-06-28 17:37:42 IST	2023-06-28 17:37:42 IST	2023-06-28 09:45:00 IST
seoul-21985.mp4			1	2023-04-25 16:40:34 IST	2023-06-28 17:55:41 IST	2023-06-28 17:55:41 IST	2023-05-05 11:48:41 IST
waterfall-37088.mp4			1	2023-04-25 16:39:47 IST	2023-06-28 17:55:47 IST	2023-06-28 17:55:47 IST	2023-05-05 11:48:41 IST
yellow-gc0037196e_1920.jpg			0	2023-04-25 16:38:20 IST	2023-06-28 17:56:08 IST	2023-06-28 17:56:08 IST	2023-05-05 11:48:41 IST
~$e drive.docx			0	2023-06-28 09:45:01 IST	2023-06-28 10:40:59 IST	2023-06-28 17:56:09 IST	2023-06-28 09:45:01 IST

Figure 113all deleted and move files

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2023-06-28 13:46:56 IST	2023-06-28 13:46:56 IST	2023-06-28 17:56:09 IST	2023-06-28 10:39:53 IST
[parent folder]				2023-06-28 11:57:59 IST	2023-06-28 11:57:59 IST	2023-06-28 19:48:15 IST	2023-06-25 20:05:36 IST
Custom Office Templates				2023-06-28 10:40:59 IST	2023-06-28 10:41:15 IST	2023-06-28 17:56:09 IST	2023-06-28 10:40:59 IST
photos				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
desktop.ini			0	2023-06-28 13:46:56 IST	2023-06-28 13:46:57 IST	2023-06-28 19:48:23 IST	2023-06-25 20:03:22 IST
Self Photo.jpg				2023-06-28 11:30:30 IST	2023-06-28 11:30:30 IST	2023-06-28 11:30:29 IST	2023-06-25 17:13:03 IST

Figure 114deleted files from one drive

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)	Known	Location
[current folder]				2023-06-28 10:41:21 IST	2023-06-28 10:41:21 IST	2023-06-28 17:30:32 IST	2023-06-25 20:03:17 IST	48	Allocated	Allocated	unknown	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/Desktop/.
[parent folder]				2023-06-28 10:41:00 IST	2023-06-28 10:41:00 IST	2023-06-28 17:42:21 IST	2023-06-25 20:03:17 IST	256	Allocated	Allocated	unknown	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/Desktop/.

Figure 115Real Desktop image

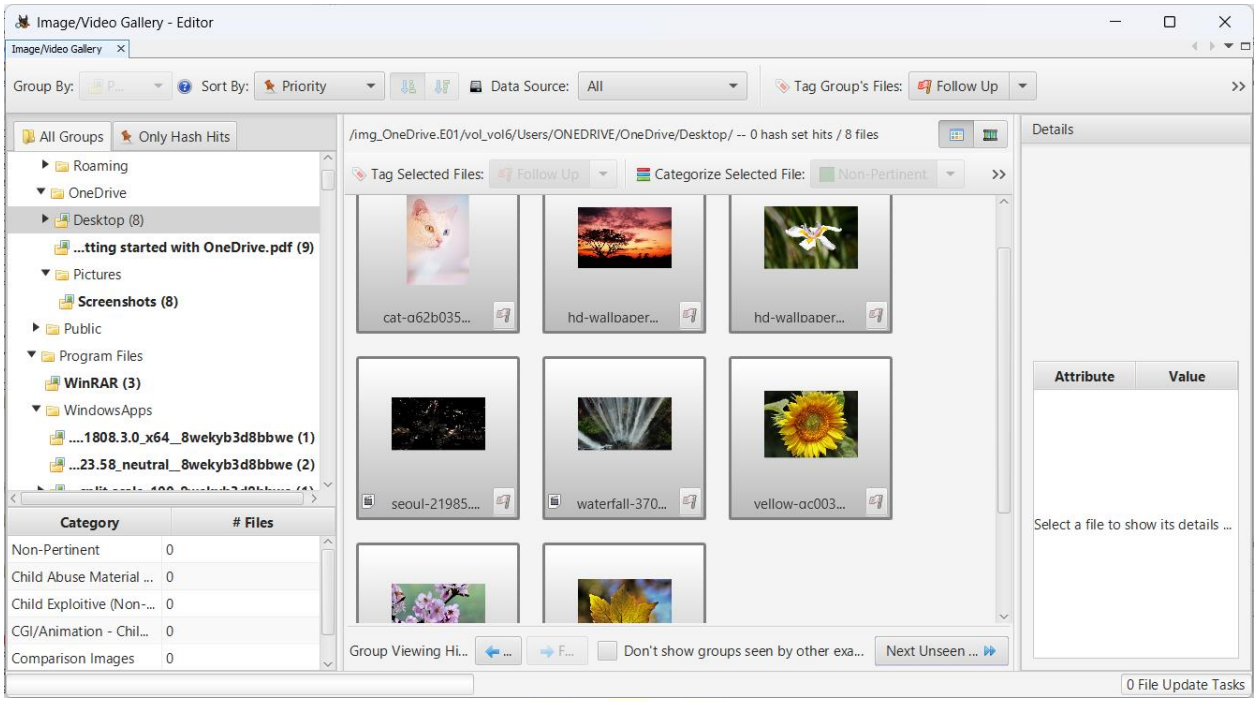


Figure 116all the image in one drive

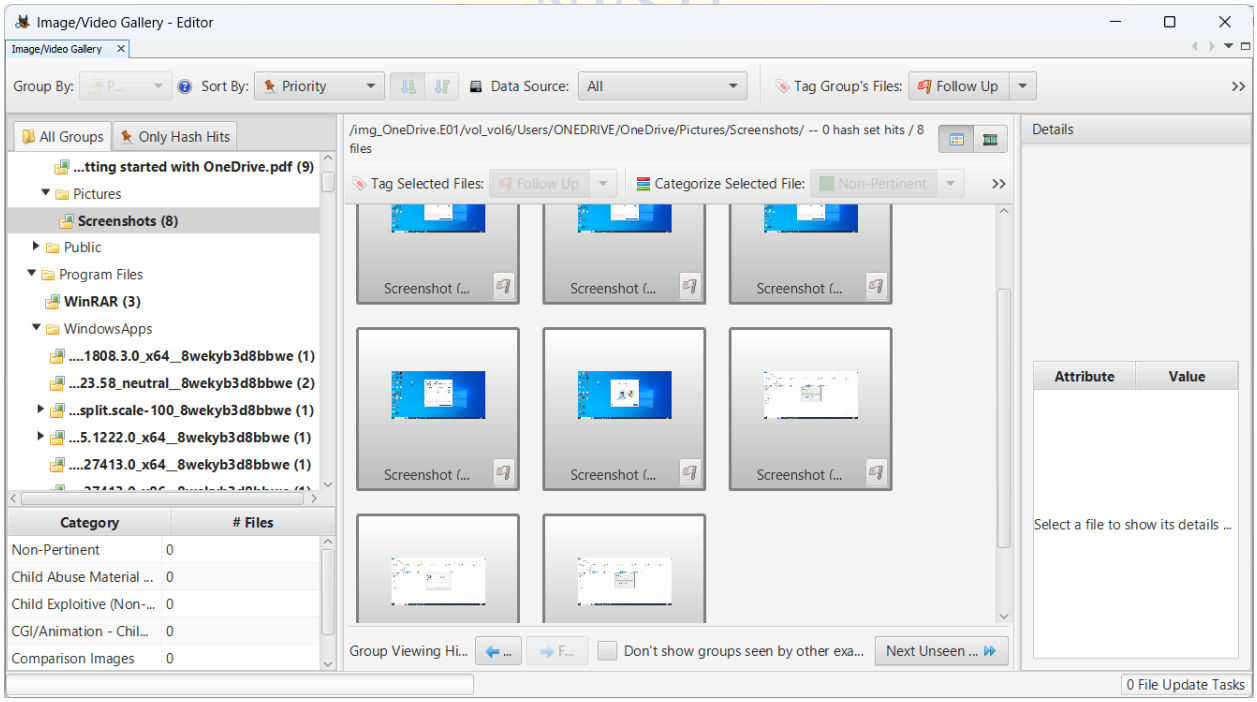


Figure 117screenshort found

We can find all the image are there in the drive with all screen short and all are deleted from the drive

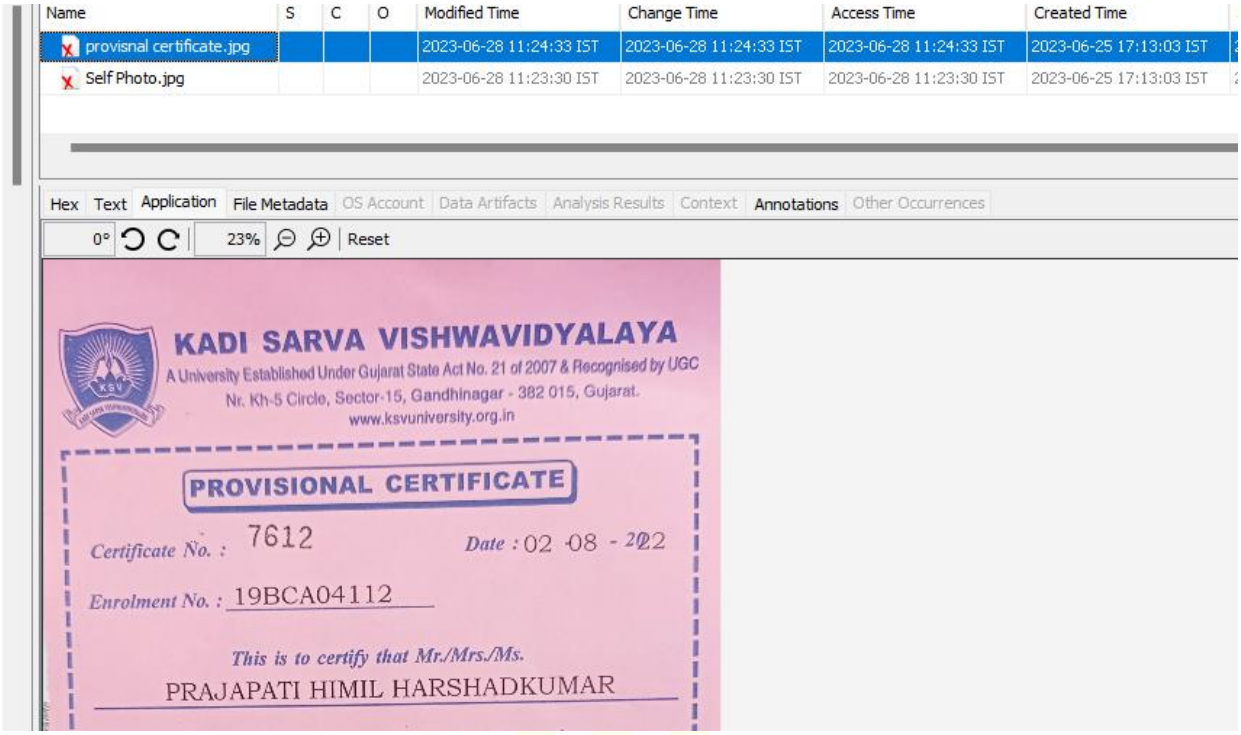


Figure 118Deleted files on Cloud

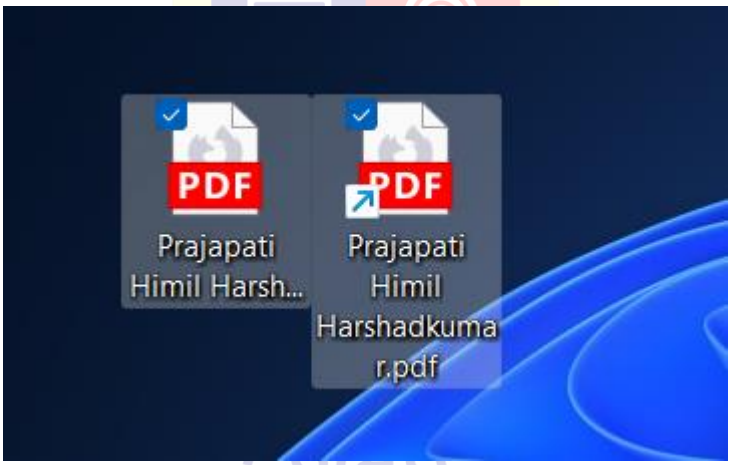


Figure 119Scuccess fully recovered files

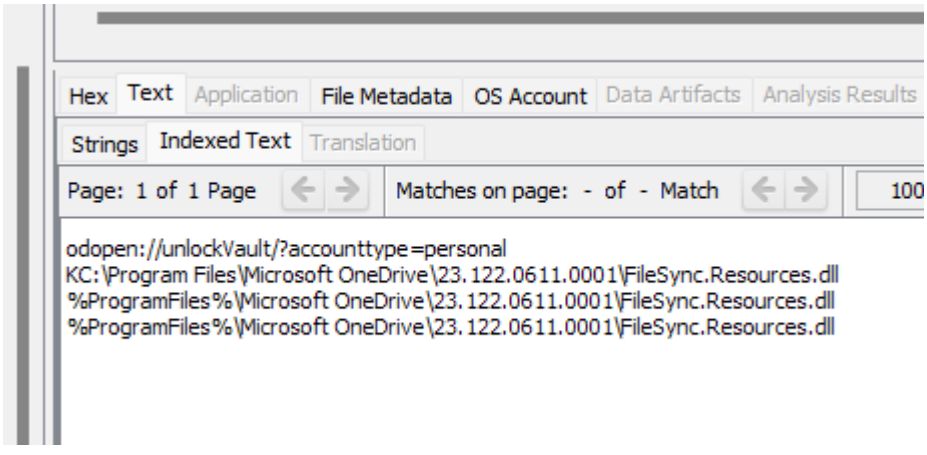


Figure 120One drive used Dll files

Vault use this files

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Eula.txt				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-26 00:49:44 IST	2022-10-26 18:50:10 IST
Eula.txt-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-26 00:49:44 IST	2022-10-26 18:50:10 IST
Logfile.PML				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:06 IST	2023-06-24 18:52:19 IST
Logfile.PML-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:06 IST	2023-06-24 18:52:19 IST
procmon.chm				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:06 IST	2022-10-26 18:50:52 IST
procmon.chm-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:06 IST	2022-10-26 18:50:52 IST
Procmon.exe				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
Procmon.exe-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
Procmon64.exe				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
Procmon64.exe-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
Procmon64a.exe				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
Procmon64a.exe-slack				2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST

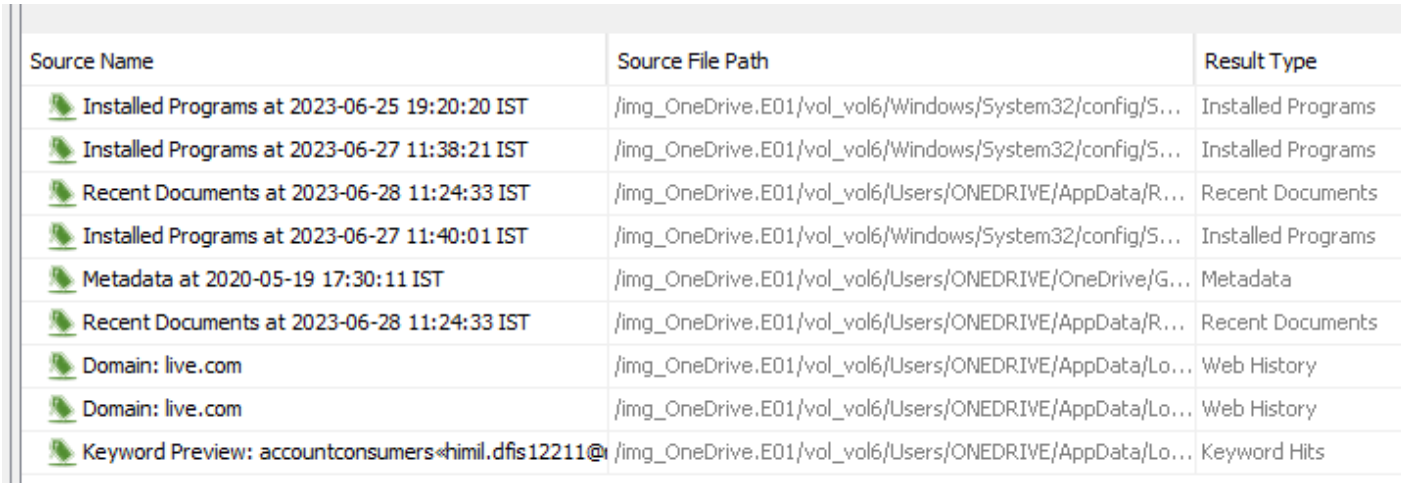
Figure 121 files are deleted

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

14.5 Browser artifact

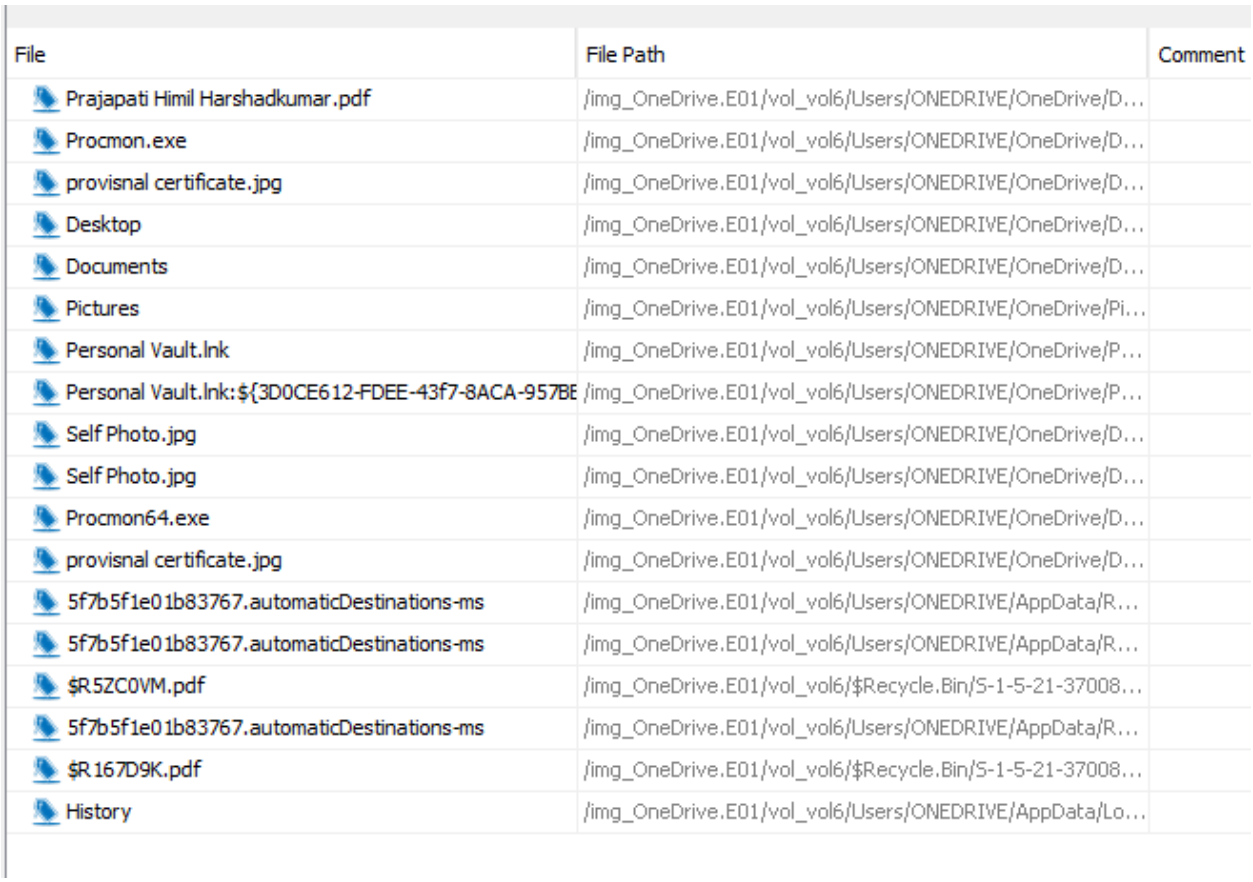
Source Name	S	C	O	URL	Program Name	Domain	Username	Data Sourc
WebCacheV01.dat				file:///C:/Windows/system32/oobe/FirstLogonAnim.html	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat			1	https://login.live.com/oauth20_desktop.srf?lc=1033	Microsoft Edge Analyzer	live.com	ONEDRIVE	OneDrive.E
WebCacheV01.dat			1	https://login.live.com/oauth20_logout.srf?client_id=00000...	Microsoft Edge Analyzer	live.com	ONEDRIVE	OneDrive.E
WebCacheV01.dat			1	https://login.live.com/oauth20_authorize.srf?client_id=000...	Microsoft Edge Analyzer	live.com	ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Desktop/SAMPLE%20STUFF/HI...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Desktop/SAMPLE%20STUFF/HI...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				ms-gamingoverlay://kglcheck/	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				ms-gamingoverlay:///	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Desktop/One%20drive.docx	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat			1	https://odc.officeapps.live.com/odc/v2.1/hrd?app=14&p...	Microsoft Edge Analyzer	live.com	ONEDRIVE	OneDrive.E
WebCacheV01.dat			1	https://odc.officeapps.live.com/odc/v2.1/hrd?app=14&p...	Microsoft Edge Analyzer	live.com	ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Pictures/Screenshots/Screensh...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Pictures/Screenshots/Screensh...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Pictures/Screenshots/Screensh...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/Pictures/Screenshots/Screensh...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/OneDrive/Pictures/Screenshots...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/OneDrive/Desktop/One%20driv...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/OneDrive/Desktop/memdump.m...	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E
WebCacheV01.dat				file:///C:/Users/ONEDRIVE/OneDrive/Desktop/doc	Microsoft Edge Analyzer		ONEDRIVE	OneDrive.E

Figure 122browser history



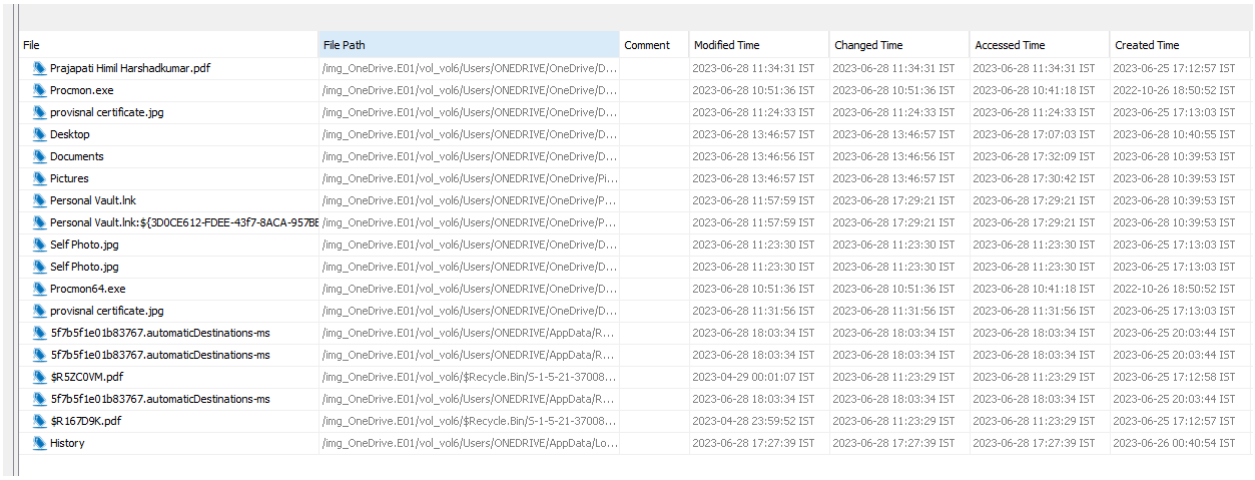
Source Name	Source File Path	Result Type
Installed Programs at 2023-06-25 19:20:20 IST	/img_OneDrive.E01/vol_vol6/Windows/System32/config/S...	Installed Programs
Installed Programs at 2023-06-27 11:38:21 IST	/img_OneDrive.E01/vol_vol6/Windows/System32/config/S...	Installed Programs
Recent Documents at 2023-06-28 11:24:33 IST	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...	Recent Documents
Installed Programs at 2023-06-27 11:40:01 IST	/img_OneDrive.E01/vol_vol6/Windows/System32/config/S...	Installed Programs
Metadata at 2020-05-19 17:30:11 IST	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/G...	Metadata
Recent Documents at 2023-06-28 11:24:33 IST	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...	Recent Documents
Domain: live.com	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Lo...	Web History
Domain: live.com	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Lo...	Web History
Keyword Preview: accountconsumers«himil.dfis12211@	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Lo...	Keyword Hits

Figure 123book mark of all evidence



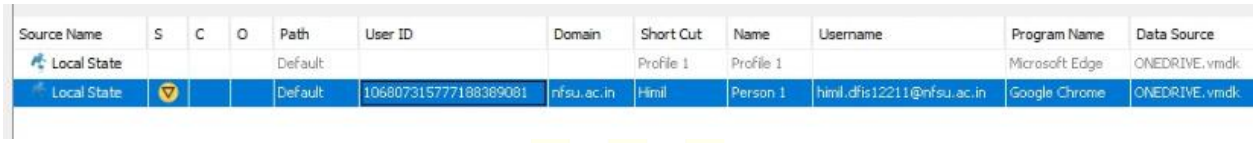
File	File Path	Comment
Prajapati Himil Harshadkumar.pdf	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Procmon.exe	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
provisnal certificate.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Desktop	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Documents	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Pictures	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/Pi...	
Personal Vault.lnk	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/P...	
Personal Vault.lnk:${3D0CE612-FDEE-43f7-8ACA-957BE	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/P...	
Self Photo.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Self Photo.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
Procmon64.exe	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
provisnal certificate.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...	
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...	
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...	
$R5ZC0VM.pdf	/img_OneDrive.E01/vol_vol6/$Recycle.Bin/S-1-5-21-37008...	
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...	
$R167D9K.pdf	/img_OneDrive.E01/vol_vol6/$Recycle.Bin/S-1-5-21-37008...	
History	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Lo...	

Figure 124Book mark list



File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time
Prajapati Himil Harshadkumar.pdf	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 11:34:31 IST	2023-06-28 11:34:31 IST	2023-06-28 11:34:31 IST	2023-06-25 17:12:57 IST
Procmon.exe	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
provisnal certificate.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 11:24:33 IST	2023-06-28 11:24:33 IST	2023-06-28 11:24:33 IST	2023-06-25 17:13:03 IST
Desktop	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 13:46:57 IST	2023-06-28 13:46:57 IST	2023-06-28 17:07:03 IST	2023-06-28 10:40:55 IST
Documents	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 13:46:56 IST	2023-06-28 13:46:56 IST	2023-06-28 17:32:09 IST	2023-06-28 10:39:53 IST
Pictures	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/Pi...		2023-06-28 13:46:57 IST	2023-06-28 13:46:57 IST	2023-06-28 17:30:42 IST	2023-06-28 10:39:53 IST
Personal Vault.lnk	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/P...		2023-06-28 11:57:59 IST	2023-06-28 17:29:21 IST	2023-06-28 17:29:21 IST	2023-06-28 10:39:53 IST
Personal Vault.lnk:${3D0CE612-FDEE-43f7-8ACA-957BE	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/P...		2023-06-28 11:57:59 IST	2023-06-28 17:29:21 IST	2023-06-28 17:29:21 IST	2023-06-28 10:39:53 IST
Self Photo.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 11:23:30 IST	2023-06-28 11:23:30 IST	2023-06-28 11:23:30 IST	2023-06-25 17:13:03 IST
Self Photo.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 11:23:30 IST	2023-06-28 11:23:30 IST	2023-06-28 11:23:30 IST	2023-06-25 17:13:03 IST
Procmon64.exe	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 10:51:36 IST	2023-06-28 10:51:36 IST	2023-06-28 10:41:18 IST	2022-10-26 18:50:52 IST
provisnal certificate.jpg	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/OneDrive/D...		2023-06-28 11:31:56 IST	2023-06-28 11:31:56 IST	2023-06-28 11:31:56 IST	2023-06-25 17:13:03 IST
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...		2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-25 20:03:44 IST
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...		2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-25 20:03:44 IST
$R5ZC0VM.pdf	/img_OneDrive.E01/vol_vol6/$Recycle.Bin/S-1-5-21-37008...		2023-04-29 00:01:07 IST	2023-06-28 11:23:29 IST	2023-06-28 11:23:29 IST	2023-06-25 17:12:58 IST
5f7b5f1e01b83767.automaticDestinations-ms	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/R...		2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-28 18:03:34 IST	2023-06-25 20:03:44 IST
$R167D9K.pdf	/img_OneDrive.E01/vol_vol6/$Recycle.Bin/S-1-5-21-37008...		2023-04-28 23:59:52 IST	2023-06-28 11:23:29 IST	2023-06-28 11:23:29 IST	2023-06-25 17:12:57 IST
History	/img_OneDrive.E01/vol_vol6/Users/ONEDRIVE/AppData/Lo...		2023-06-28 17:27:39 IST	2023-06-28 17:27:39 IST	2023-06-28 17:27:39 IST	2023-06-26 00:40:54 IST

Figure 125Book marks and history



Source Name	S	C	O	Path	User ID	Domain	Short Cut	Name	Username	Program Name	Data Source
Local State				Default			Profile 1	Profile 1		Microsoft Edge	ONEDRIVE.vmdk
Local State				Default	106807315777188389081	nfsu.ac.in	Himil	Person 1	himil.dfis12211@nfsu.ac.in	Google Chrome	ONEDRIVE.vmdk

Figure 126Email ID found profile

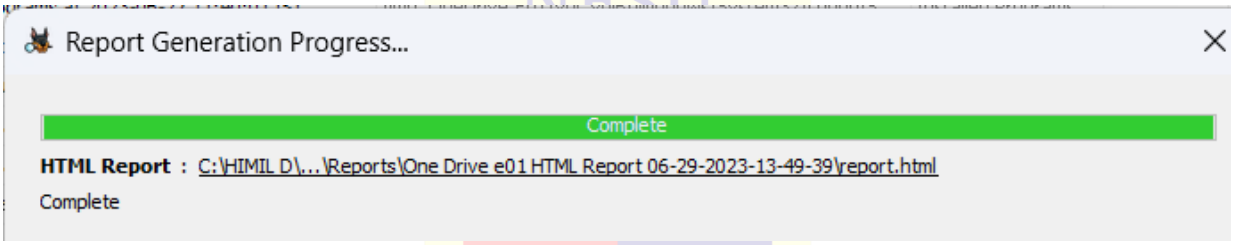


Figure 127creted successfully report

14.6 Live browser artifact

site setting (modif	2023-06-27 21:33:37.416	https://www.google.com:443,*	media_engagement [in Prefe	{'expiration': '13340176417416227', 'last_modified
site setting (hsts)	2023-06-27 21:33:40.854	Encoded domain: HPKF08Y4Ny21MnLunbMahM4qupMHq7pIiZjhckE+	HSTS observed	{'expiry': 1719462820.854189, 'host': 'HPKF08Y4Ny
url	2023-06-27 21:33:44.031	https://go.microsoft.com/fwlink/p/?LinkID=2147560&clcid=0x4009&	Create account	
url	2023-06-27 21:33:44.031	https://onedrive.live.com/signup	Create account	
url	2023-06-27 21:33:44.031	https://signup.live.com/signup.aspx?id=250206&wreply=https%3a%	Create account	
url	2023-06-27 21:33:44.031	https://signup.live.com/signup?id=250206&wreply=https%3a%2f%2f	Create account	
url	2023-06-27 21:33:44.031	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&checkda=	Create account	
url	2023-06-27 21:33:44.031	https://signup.live.com/signup?id=250206&wreply=https%3a%2f%2f	Create account	
site setting (hsts)	2023-06-27 21:33:45.112	Encoded domain: tXjOdUMSBgtiUbrbGkI6XP80fiDB8uXOkUbnCf0IKvw	HSTS observed	{'expiry': 1719462825.112309, 'host': 'tXjOdUMSBg
site setting (hsts)	2023-06-27 21:33:45.860	Encoded domain: 9jFJneXMVHTXLZTJwwlFuScHMcN/99brFSgqRKTizG	HSTS observed	{'expiry': 1719462825.860292, 'host': '9jFJneXMVH
site setting (hsts)	2023-06-27 21:33:47.555	Encoded domain: 04KAKyV2saGVcb3JhJ/Ne+BV6drxDYFbIEjHTVIyQ2k	HSTS observed	{'expiry': 1688013227.555972, 'host': '04KAKyV2sa
site setting (hsts)	2023-06-27 21:33:49.706	Encoded domain: XkkkB2ofzfdQ3XFACyPJHT0+0YfxhedJOx4t3KIByk8=	HSTS observed	{'expiry': 1688013229.706848, 'host': 'XkkkB2ofzfd
site setting (hsts)	2023-06-27 21:33:51.531	Encoded domain: ruspX6BYm6dO9irdkyplyxkjRWS6EdBcIM+yicsjbrw=	HSTS observed	{'expiry': 1719462831.531321, 'host': 'ruspX6BYm6
site setting (hsts)	2023-06-27 21:33:51.908	Encoded domain: Y1cbV6ziZu1KjdKdxBzKmgzsZCYqaDEHWONJJAo942	HSTS observed	{'expiry': 1719462831.908438, 'host': 'Y1cbV6ziZu1
site setting (hsts)	2023-06-27 21:33:54.558	Encoded domain: sc7YTQK1Tr64ftenpAzkUjtjhlwFP1eW2etQqyqgSEk=	HSTS observed	{'expiry': 1703478834.55888, 'host': 'sc7YTQK1Tr64
site setting (hsts)	2023-06-27 21:33:56.164	Encoded domain: 3VNxcaT4BfWg+I3FIQt0pE1XpIsbUMiPGUhLOgHMn	HSTS observed	{'expiry': 1719462836.164959, 'host': '3VNxcaT4Bf
site setting (modif	2023-06-27 21:34:02.981	https://signup.live.com:443,*	formfill_metadata [in Prefer	{'last_modified': '13332400442981246', 'setting': {'
site setting (modif	2023-06-27 21:34:15.287	https://accounts.google.com:443,*	client_hints [in Preferences.]	{'last_modified': '13332400455287925', 'setting': {'
url	2023-06-27 21:34:44.779	https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzGsnl	Verify your email address - himil.dfis12211@nfsu.ac.in - National Forensic Scie	
site setting (hsts)	2023-06-27 21:34:45.218	Encoded domain: +lPeEeU664E5hmZDsz8+6O9RnpLxT6WoswFwUoLm	HSTS observed	{'expiry': 1698813285.218563, 'host': '+lPeEeU664E
site setting (hsts)	2023-06-27 21:34:55.082	Encoded domain: NYa2uODq6Gzvu7bRgMVd5ibHcz54g+15ngXsohhwc	HSTS observed	{'expiry': 1719462895.082161, 'host': 'NYa2uODq6C
site setting (hsts)	2023-06-27 21:34:56.300	signup.live.com	HSTS observed	{'expiry': 1719462896.300504, 'host': 'rsvP85efofCg
site setting (hsts)	2023-06-27 21:35:34.145	Encoded domain: CHpDto0z/pN67xkfqFHANWpTizPGJjvfo/lErmhe8lL	HSTS observed	{'expiry': 1719462934.145521, 'host': 'CHpDto0z/pf

Figure 128histroy of one drive login

Figure 129onedrive login id

1	Preferences (Default)	
2	Group / Setting Name	Value
3	Account Information	
4	account_id	106807315777188389081
5	email	himil.dfis12211@nfsu.ac.in
6	full_name	Himil Prajapati
7	gaia	106807315777188389081
8	given_name	Himil
9	hd	nfsu.ac.in
10	is_supervised_child	-1

Figure 130browser username and id

20	clear_lso_data_enabled	<not present>
21	Per Host Zoom Levels	
22	Sync Settings	
23	last_poll_time	2023-06-28 04:21:13.670
24	last_synced_time	2023-06-28 04:40:19.588
25	cache_guid	GCWTiYY+6dKs6/ccQ2iWqg==
26	gaia_id	106807315777188389081
27	requested	FALSE
28		
29		

Figure 131Last poll time

15. Google drive

15.1 Introduction to google drive:-

Google Drive service is the cloud based service which is available at drive.google.com. It was introduced by Google in 2002. More than 800 million daily users, according to stats given at last year's Google I/O Conference. Google Drive provides 15 GB free user space to use. It also It offers commercial solutions (100/200/500 GB - 1/214/8/16 1B).

It works on desktop and mobile OS

All Windows Version, All Mac OS Version, Android, IOS

Testing Environment

Windows 10 64-bit Operating System

Google Chrome- Web Browser

RegShot to track the registry changes

Email Account: himildfis.12211@nfsu.ac.in

Google Drive Client: Newly Updated "3.1092.2150.0"

15.2 Installation regs

15.3 hot difference

1RegShot execution and state saving

- Start the RegShot application.
- Click 1st shot button and save the state

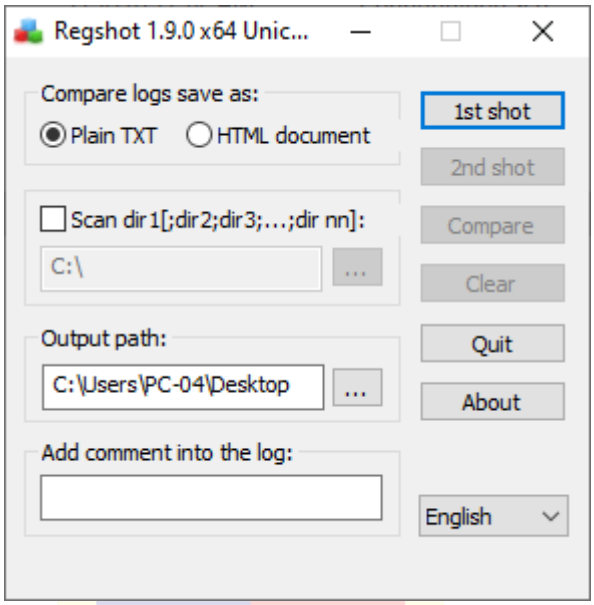


Figure 132Regshot 1

Start the client installation

- Download Google Drive online installer from Google.com.
- Now launch the installer.
- It will install Google drive automatically in your system.

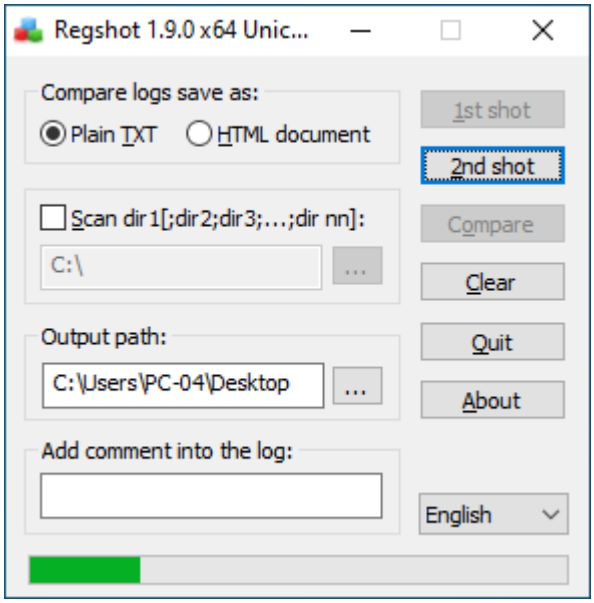


Figure 133Regshot 2

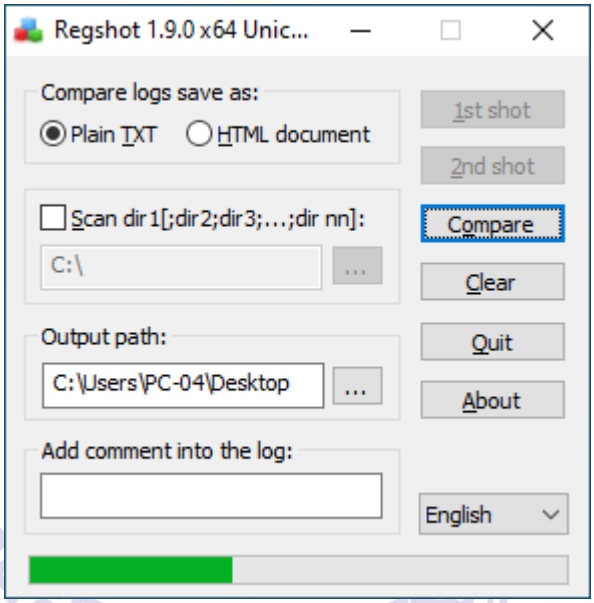


Figure 134Regshot compare

RegShot changes files

HKLM\SOFTWARE\Google\DriveFS\Driver Version: "3.1092.2150.0"

HKLM\SOFTWARE\Google\DriveFS\LastUpdateTime: 0x645A362D

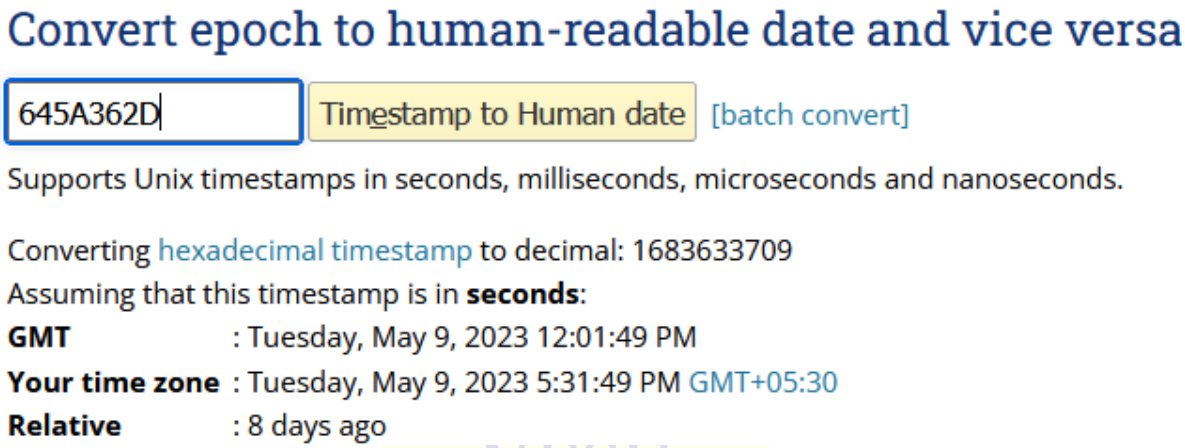


Figure 135Epoch time

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-845500802-582371313-2302652183-1000\\Device\HarddiskVolume3\Program Files\Google\Drive File Stream\73.0.4.0\GoogleDriveFS.exe: 5E F9 F4 0A 6E 82 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-845500802-582371313-2302652183-1000\\Device\HarddiskVolume3\Program Files\Google\Drive File Stream\73.0.4.0\GoogleDriveFS.exe: 43 C9 3D 34 6E 82 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00

HKLM\SOFTWARE\Classes\TypeLib\{E27EC053-3263-4908-8ECD-5AFDFB754728}\1.0\: "DriveFSExtensionLib"

HKLM\SOFTWARE\Classes\WOW6432Node\CLSID\{03E6C474-8D95-4C1B-9268-4AA3FA16DE4F}\InProcServer32\: "C:\Program Files\Google\Drive File Stream\73.0.4.0\x86\drivefsext.dll"

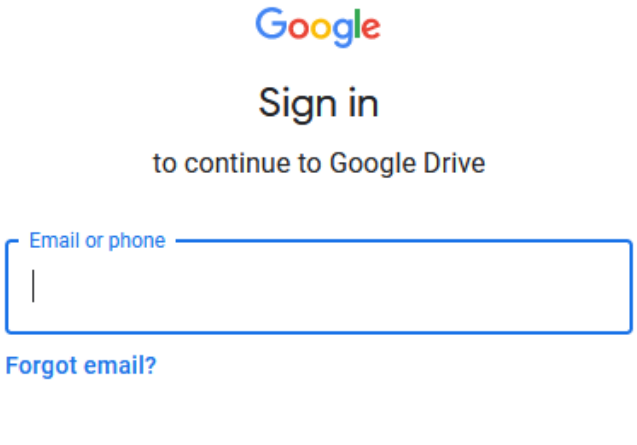


Figure 136Gdrive login page

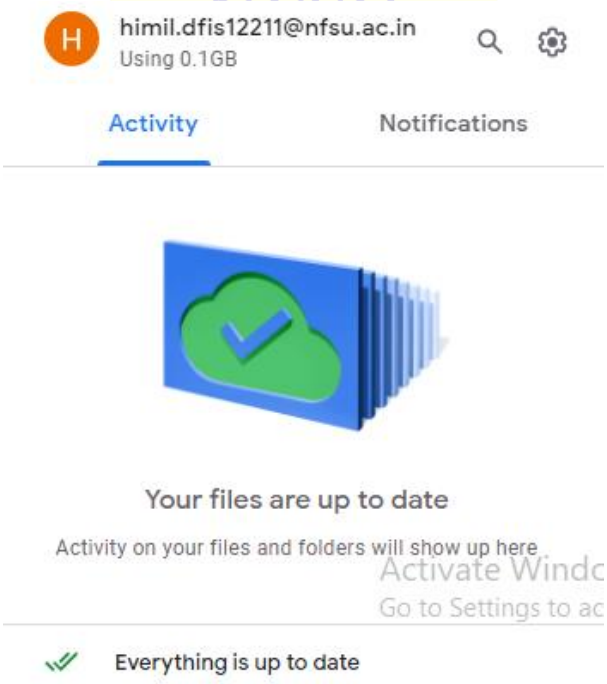


Figure 137Gdrive successfully installed

Drive is installed successfully in the local pc

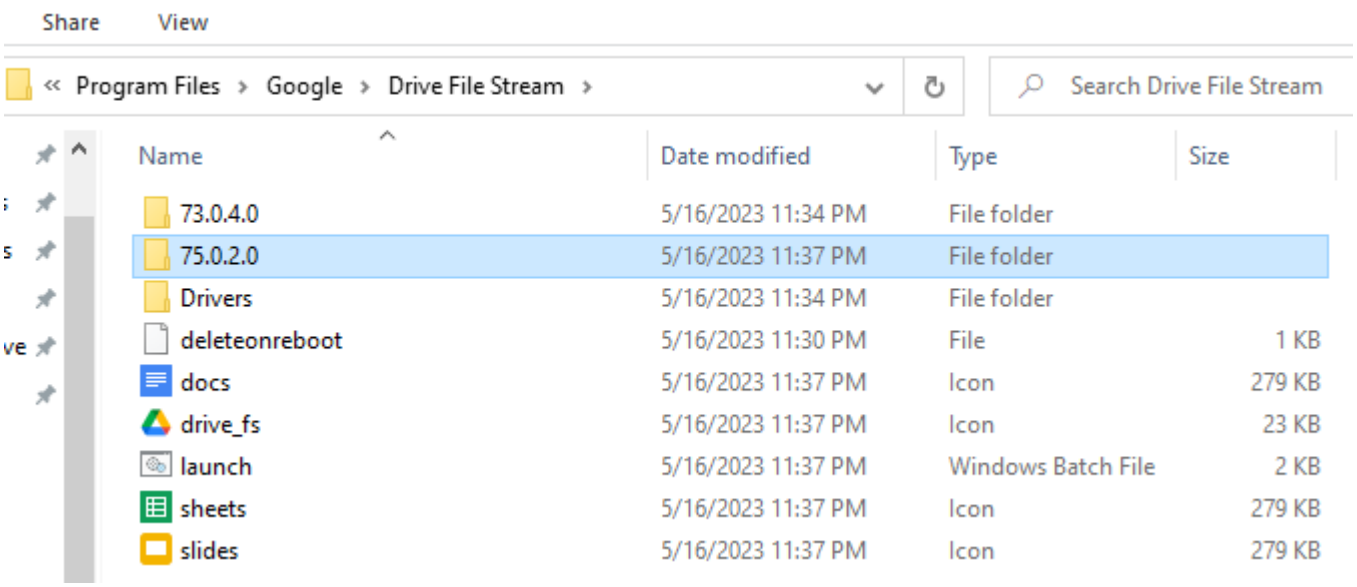


Figure 138Gdrive installed path

Google Drive Client installed inside the program file folder

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

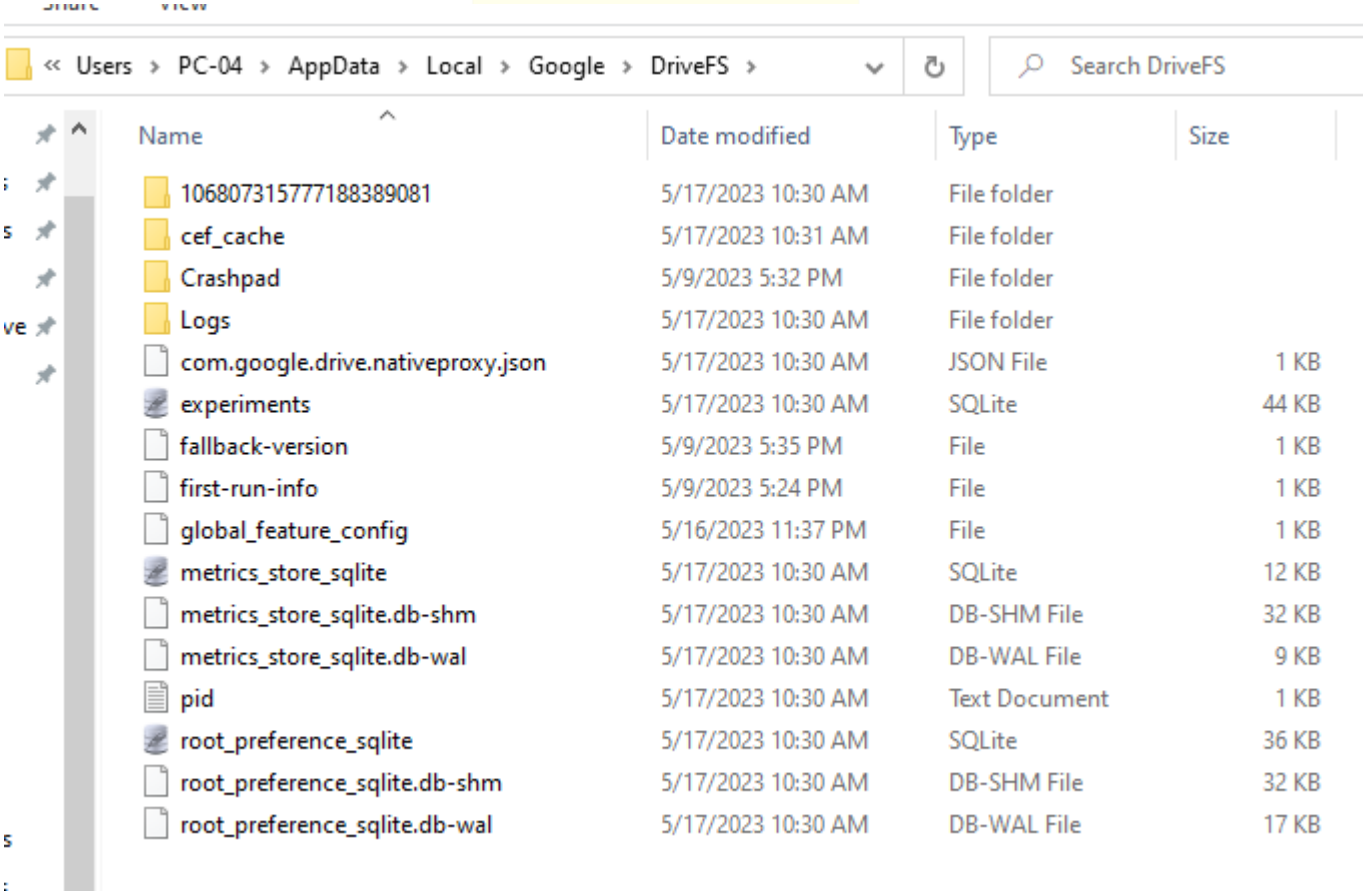


Figure 139Gdrive DB files

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\PC-04\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\PC-04\AppData\Local\Google\DriveFS\106807315777188389081”

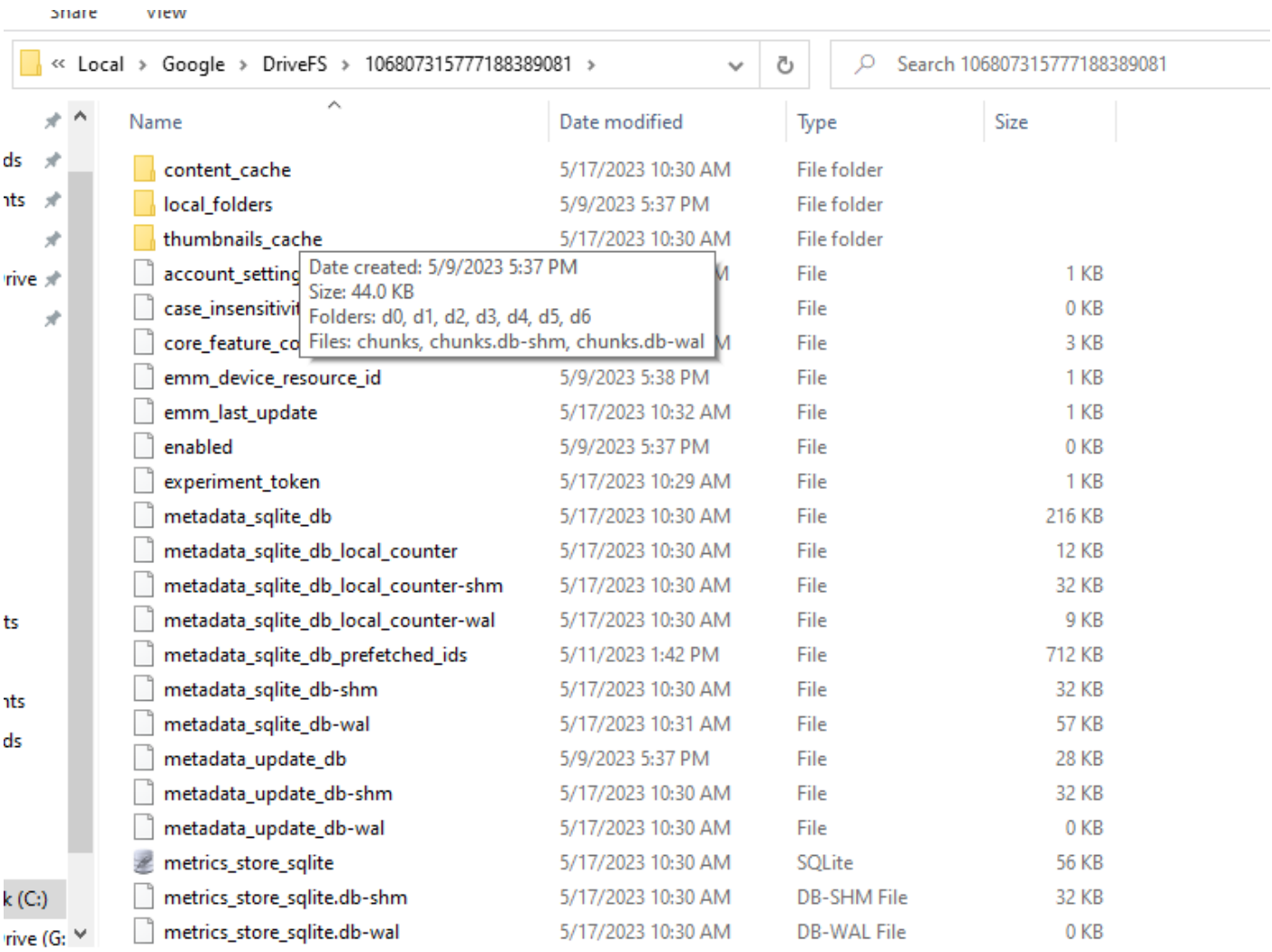


Figure 140Gdrive User Data files

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

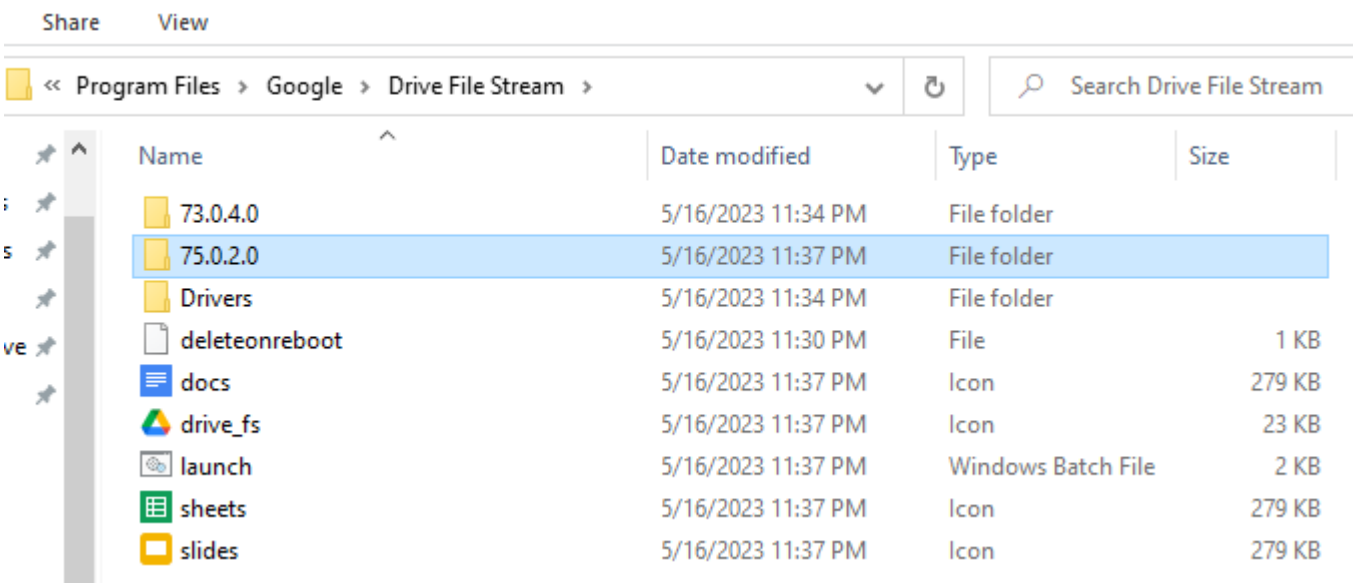


Figure 141Other files are also installed by GDrive

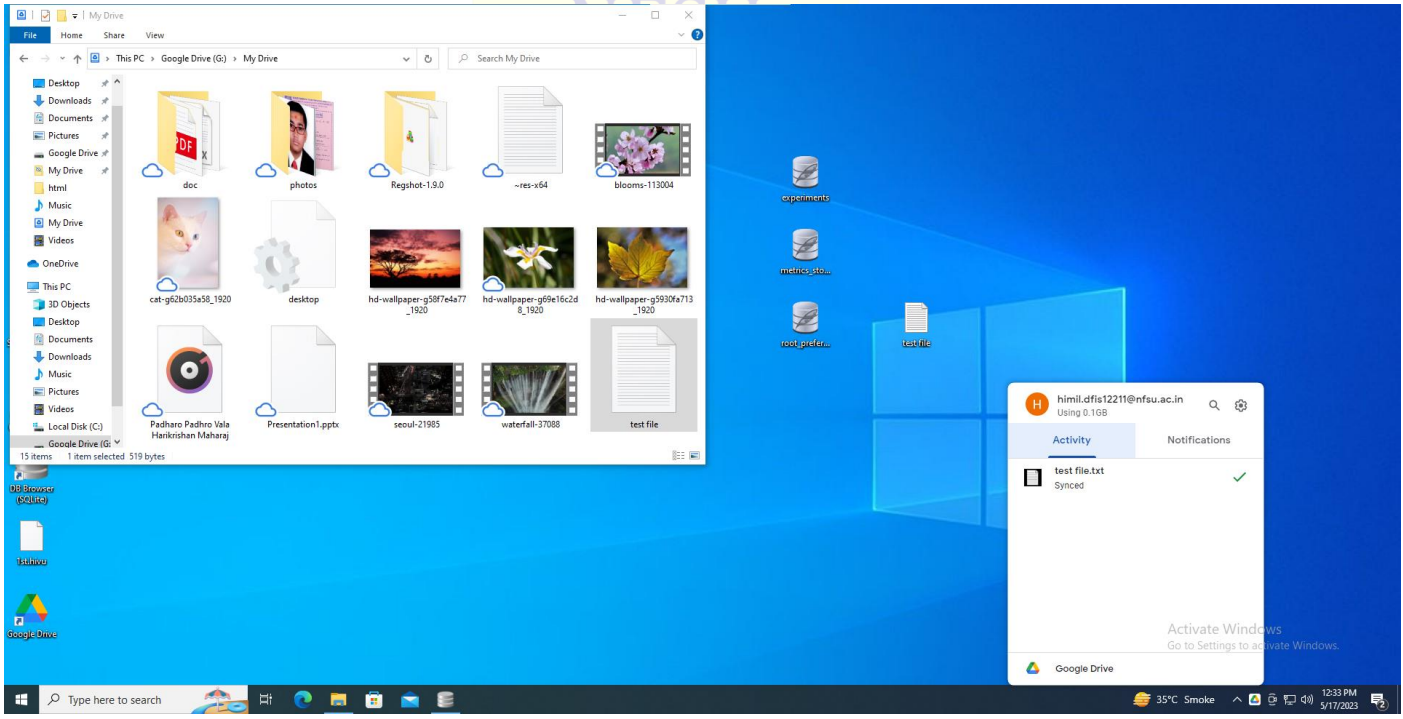


Figure 142Gdrive local Disk

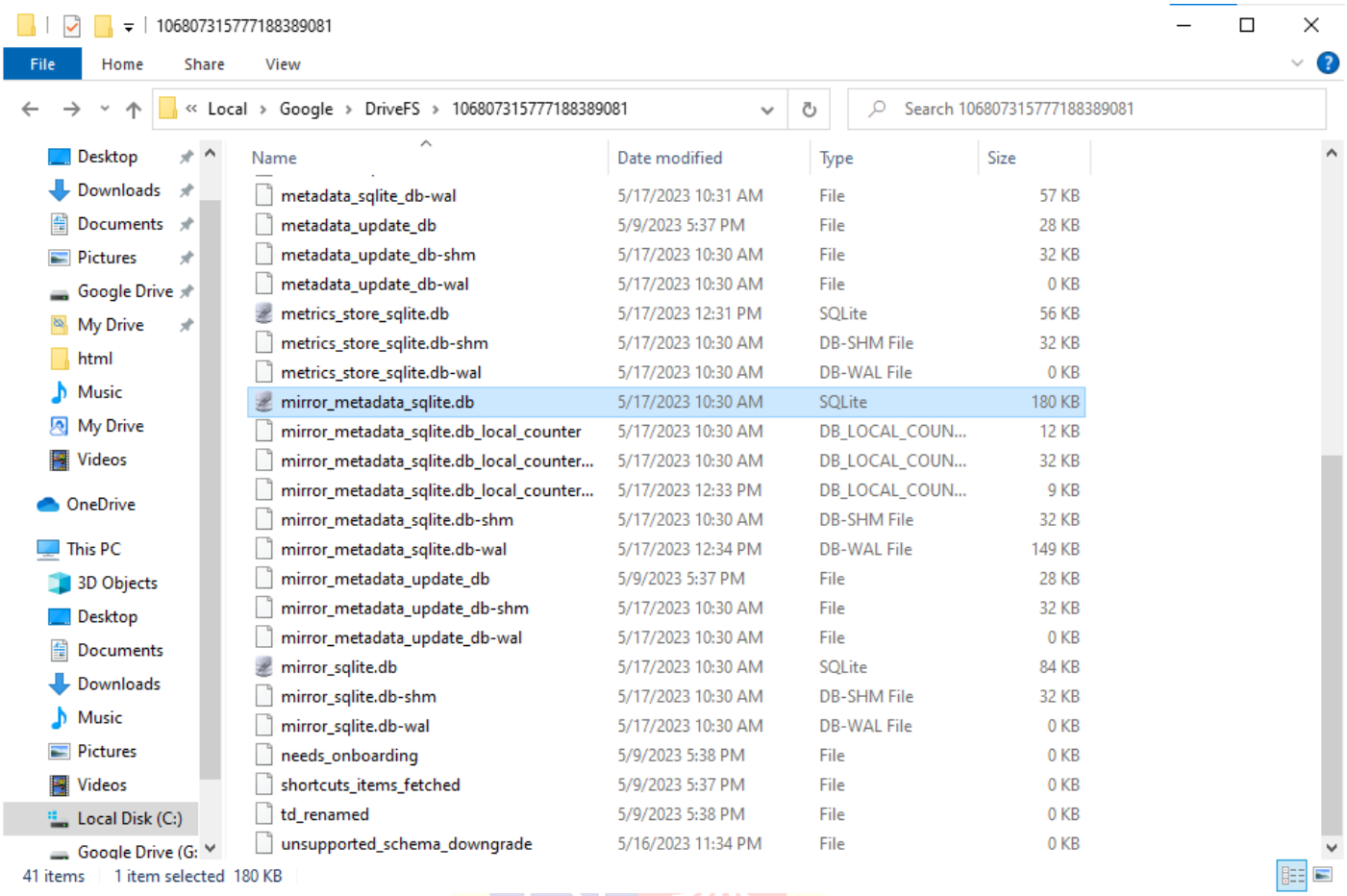


Figure 143 List of DB files created by Drive

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

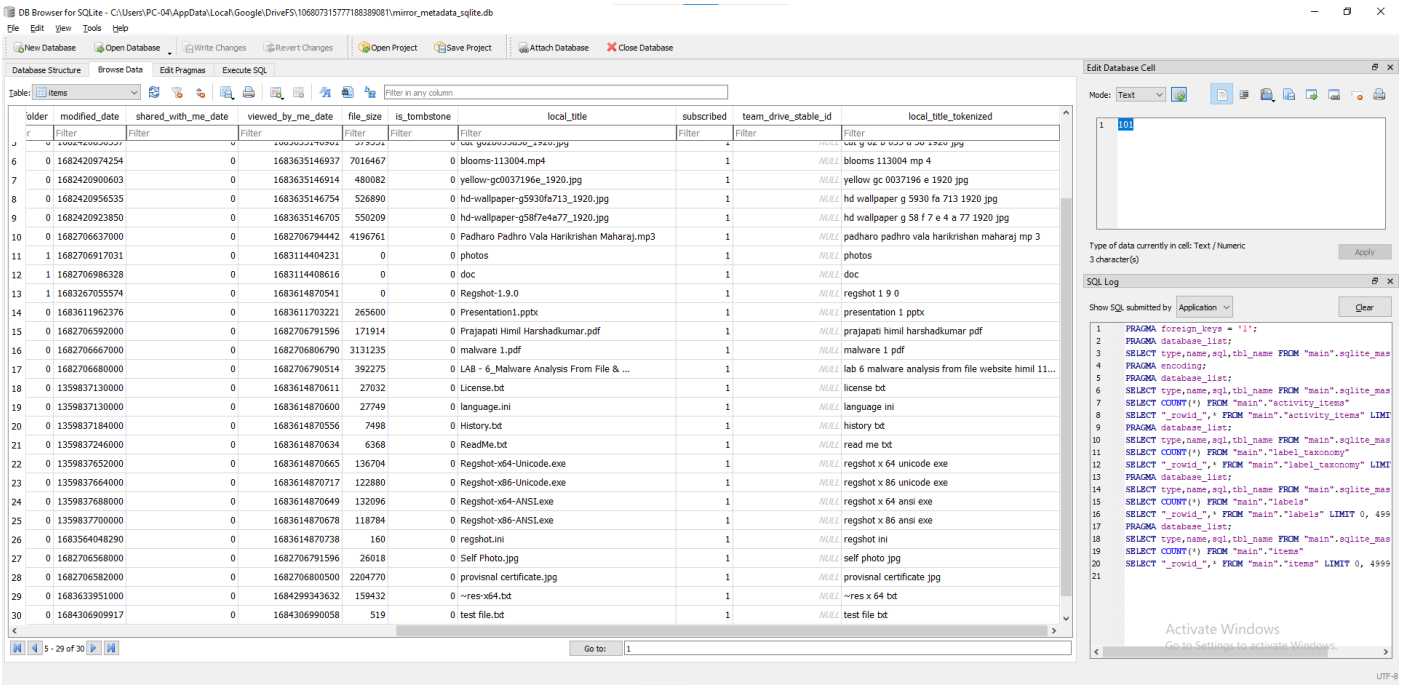


Figure 144 Sync Data entry DB file

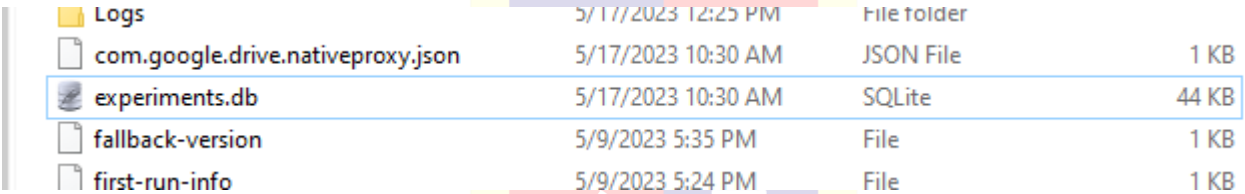


Figure 145 Data Entry Details with Epoch Time

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

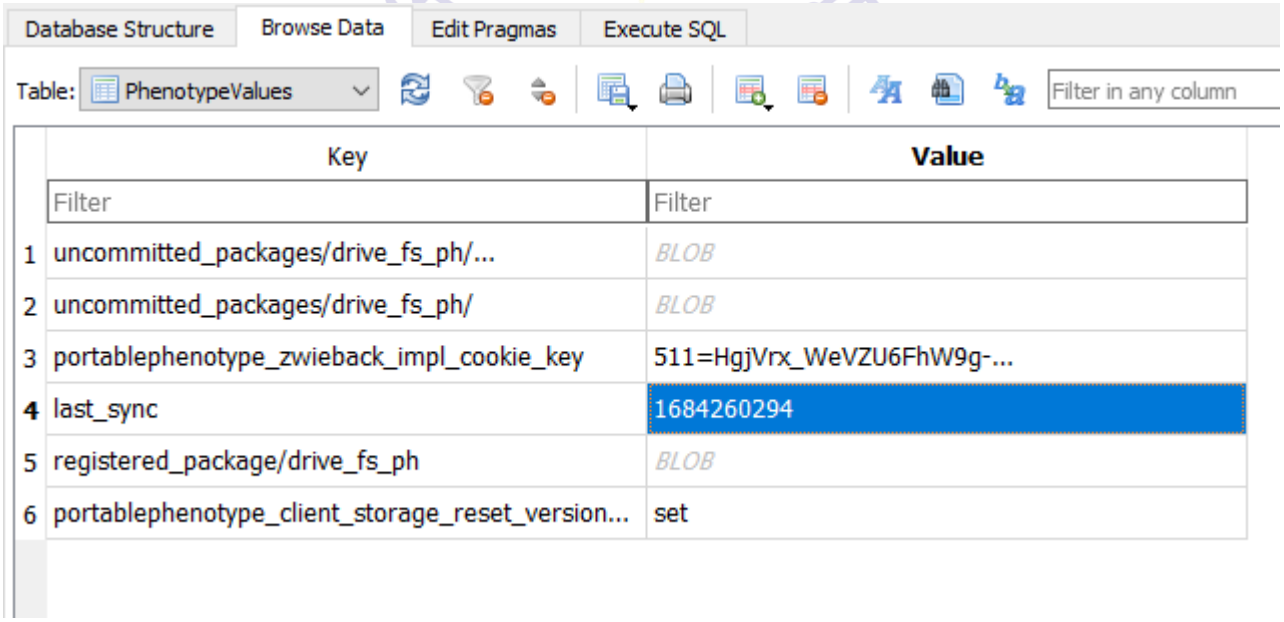


Figure 146Sync Entry DB

Figure 147File Sync Epoch Time

15.4 RAM DUMP

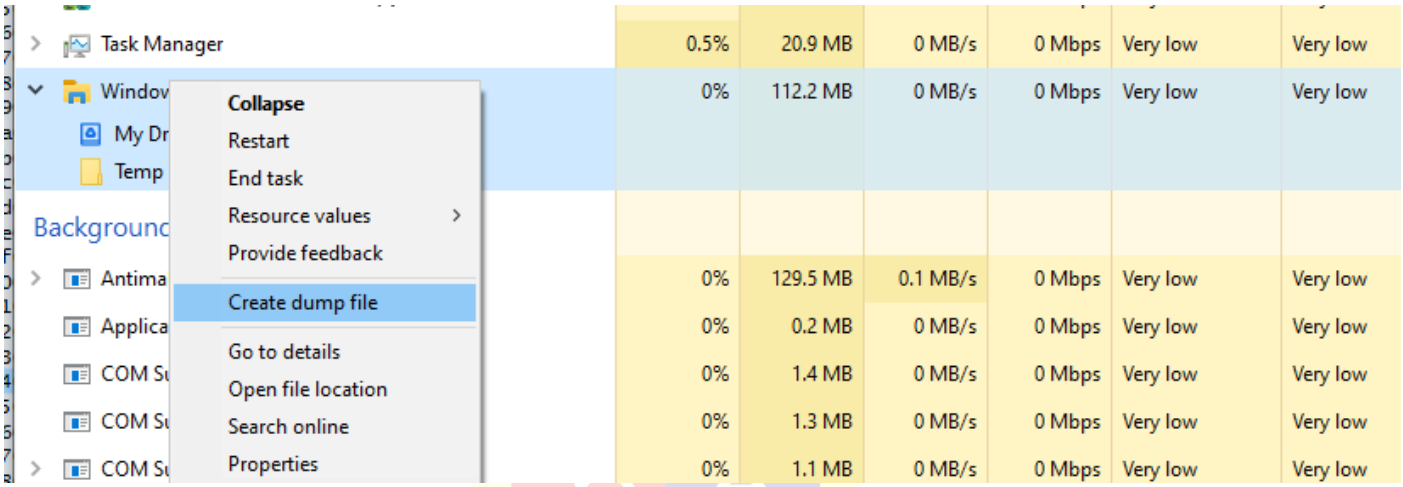


Figure 148Ram Dump through Task Manager

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

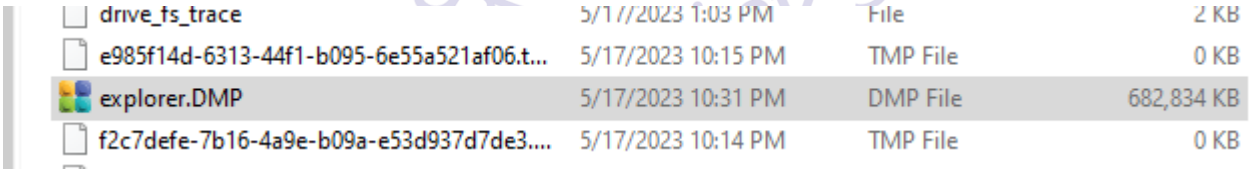


Figure 149Ram Dump Files

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

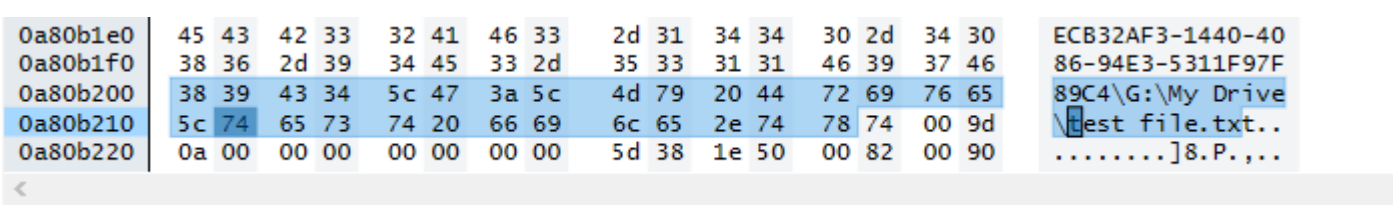


Figure 150 File Location Reveal at Sync Time

15.5 Browser side forensic

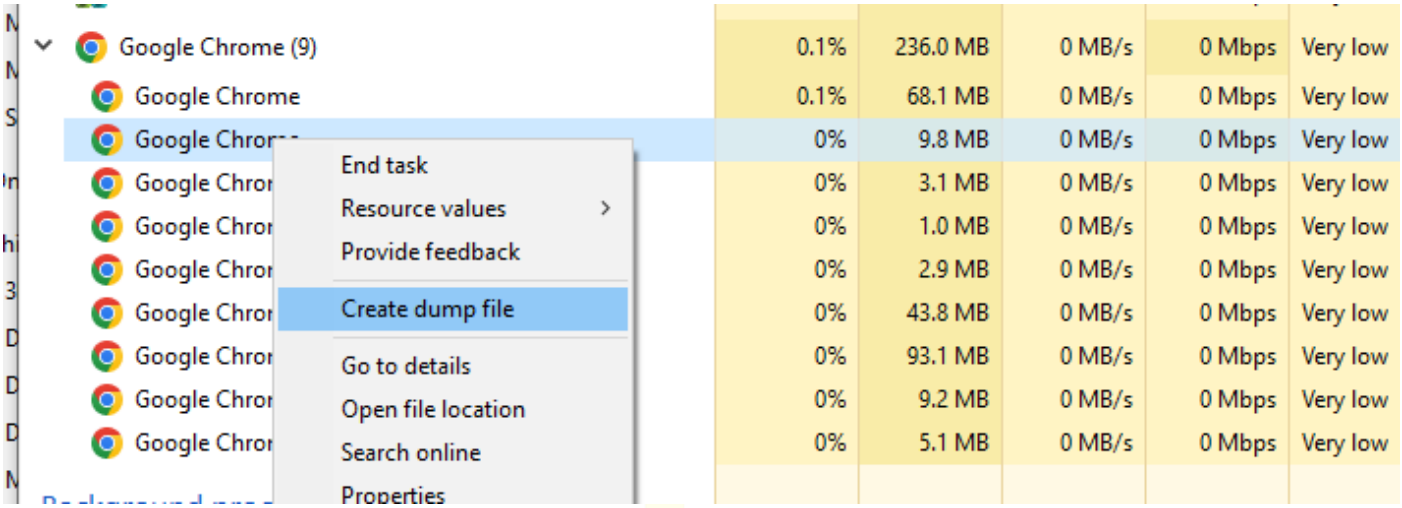


Figure 151 Dump File Created

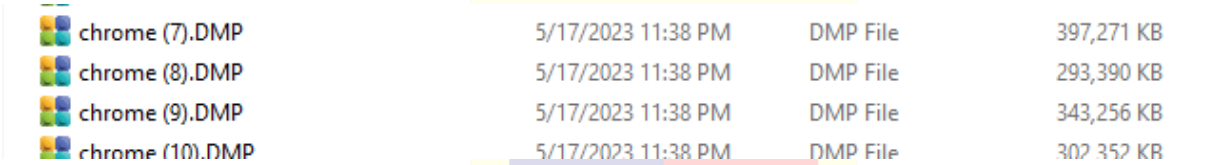


Figure 152 Dump File Stored in Temp Folder

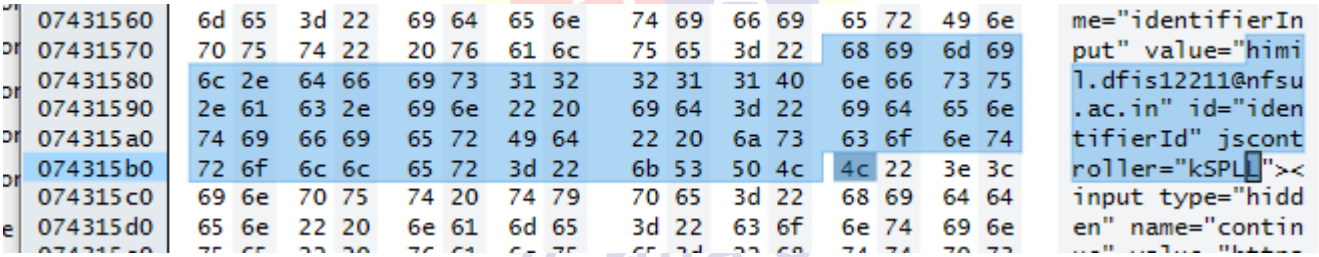


Figure 153 Email Id Retail in Ram Dump

From the browser we can successfully extracted the id and password of the user drive in plain text

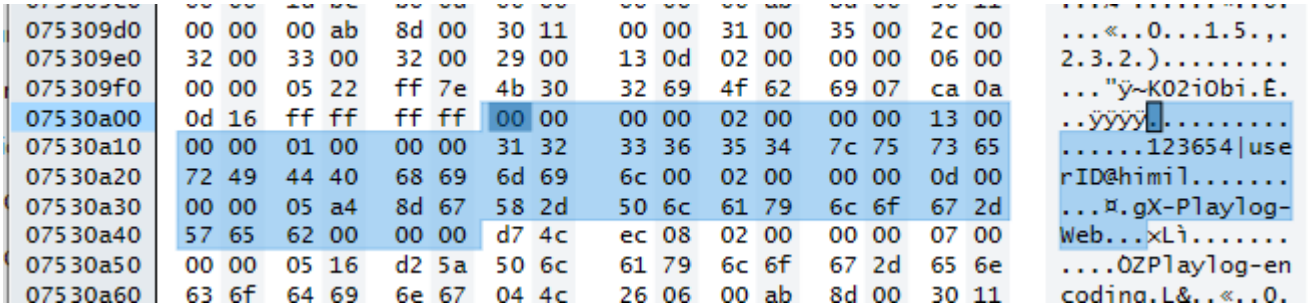


Figure 154 Password Reveal in Ram Dump

15.6 Disk analysis

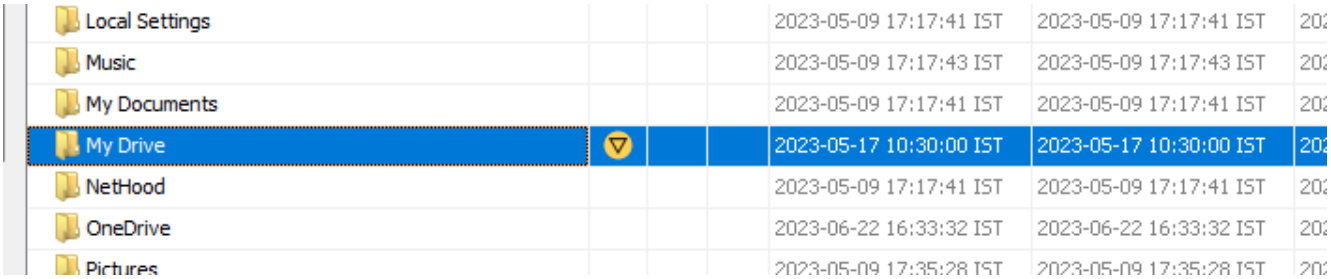


Figure 155Find GDrive location

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

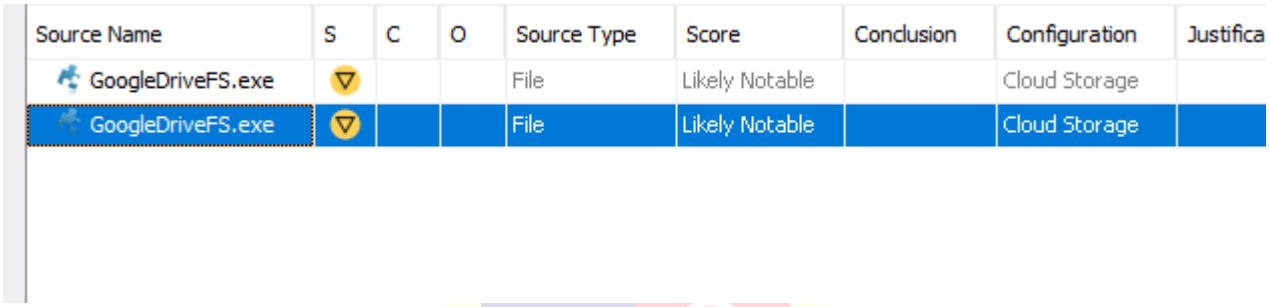


Figure 156Gdeive installed .exe

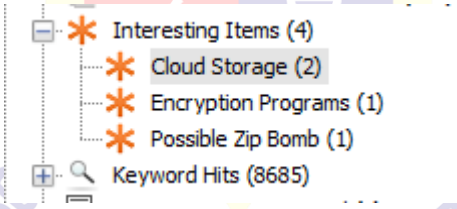


Figure 157Autopsy Suggested Cloud installed in this user

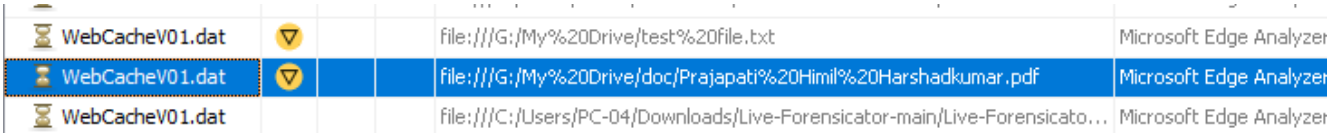


Figure 158Browser history

doc				2023-05-17 10:29:37 IST	2023-05-17 10:29:37 IST
photos				2023-05-17 10:29:37 IST	2023-05-17 10:29:37 IST
doc gshot-1.9.0				2023-05-17 10:29:37 IST	2023-05-17 10:29:37 IST
blooms-113004.mp4	▽		1	2023-04-25 16:39:34 IST	2023-05-16 23:41:28 IST
cat-g62b035a58_1920.jpg	▽		1	2023-04-25 16:37:36 IST	2023-05-16 23:41:26 IST
desktop.ini			0	2023-05-17 10:30:00 IST	2023-05-17 10:30:00 IST
hd-wallpaper-g58f7e4a77_1920.jpg	▽		2	2023-04-25 16:38:43 IST	2023-05-16 23:41:27 IST
hd-wallpaper-g5930fa713_1920.jpg	▽		2	2023-04-25 16:39:16 IST	2023-05-16 23:41:27 IST
hd-wallpaper-g69e16c2d8_1920.jpg	▽		2	2023-04-25 16:38:02 IST	2023-05-16 23:41:28 IST
Padharo Padhro Vala Harikrishan Maharaj.mp3			0	2023-04-29 00:00:37 IST	2023-05-16 23:41:27 IST
Presentation1.pptx			0	2023-05-09 11:29:22 IST	2023-05-16 23:41:27 IST
seoul-21985.mp4	▽		2	2023-04-25 16:40:34 IST	2023-05-16 23:41:30 IST
waterfall-37088.mp4	▽		1	2023-04-25 16:39:47 IST	2023-05-16 23:41:35 IST
~res-x64.txt			1	2023-05-09 17:35:51 IST	2023-05-17 10:29:38 IST

Figure 159List of all files in GDrive

metrics_store_sqlite.db-shm			2	2023-06-23 14:49:41 IST	2023-06-23 14:49:41 IS
metrics_store_sqlite.db-wal			0	2023-06-23 14:34:48 IST	2023-06-23 14:34:48 IS
mirror_metadata_sqlite.db	▽		0	2023-06-21 23:50:21 IST	2023-06-21 23:50:21 IS
mirror_metadata_sqlite.db-shm			2	2023-06-23 14:49:41 IST	2023-06-23 14:49:41 IS
mirror_metadata mirror_metadata_sqlite.db			0	2023-06-23 14:56:11 IST	2023-06-23 14:56:11 IS
mirror_metadata_sqlite.db_local_counter			0	2023-06-21 15:49:32 IST	2023-06-21 15:49:32 IS

Figure 160Sync DB

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

Table: items — 336 entries — Page 1 of 4 — Export to CSV

pe	is_folder	modified_date	shared_...	viewed_by_me...	file_size	is_tombs...	local_title	subscribed	team_dri...	local_title_tokenized
n/vnd.google-apps.folder	1	1677347305090	0	0	0	0	My Drive	1		my drive
4	mime_type	82421034043	0	1683635146776	3238956	0	seoul-21985.mp4	1		seoul 21985 mp 4
g	0	1682420882237	0	1683635146732	362830	0	hd-wallpaper-g69e16c2d8_1920.jpg	1		hd wallpaper g 69 e 16 c 2 d 8 1920 jpg
4	0	1682420987845	0	1683635146808	32026769	0	waterfall-37088.mp4	1		waterfall 37088 mp 4
g	0	1682420856537	0	1684350875992	379351	0	cat-g62b035a58_1920.jpg	1		cat g 62 b 035 a 58 1920 jpg

Figure 161all entry of sync DB

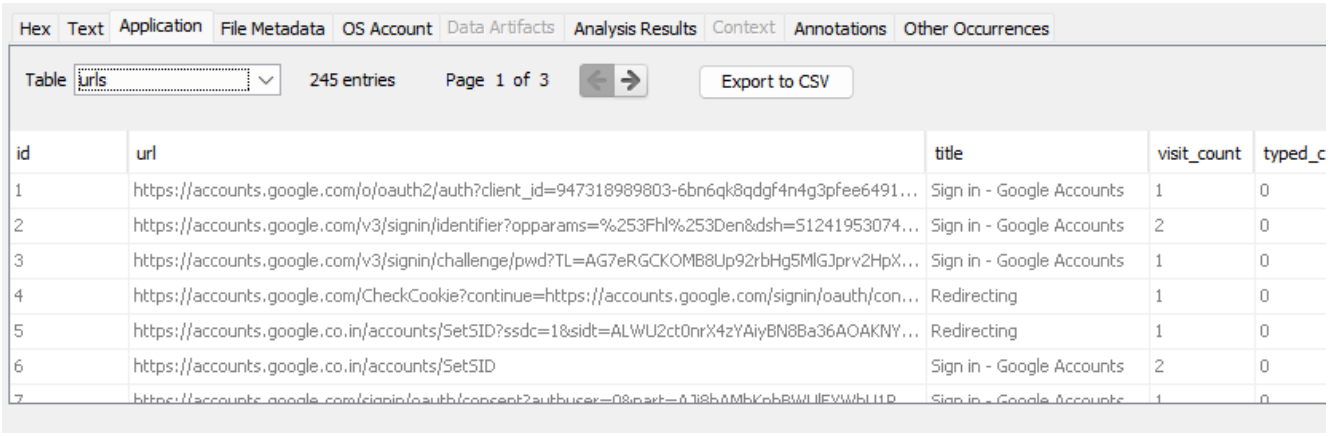


Figure 162Chrom history DB GDrive login

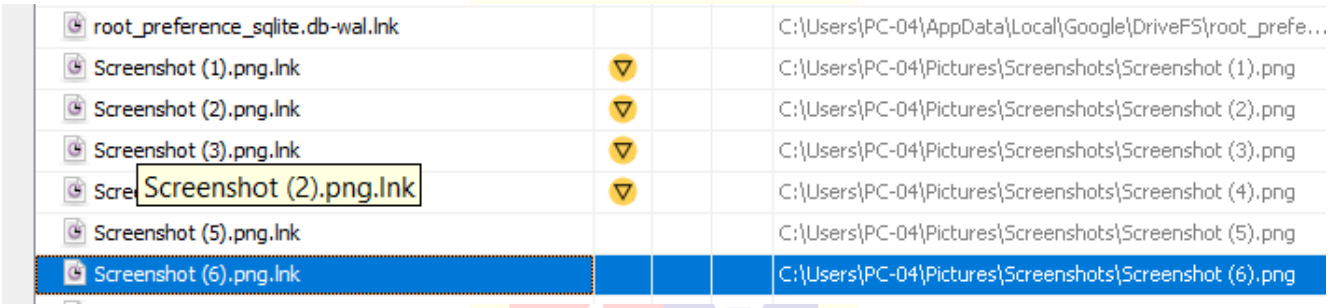


Figure 163uploaded successfully document are in lnk

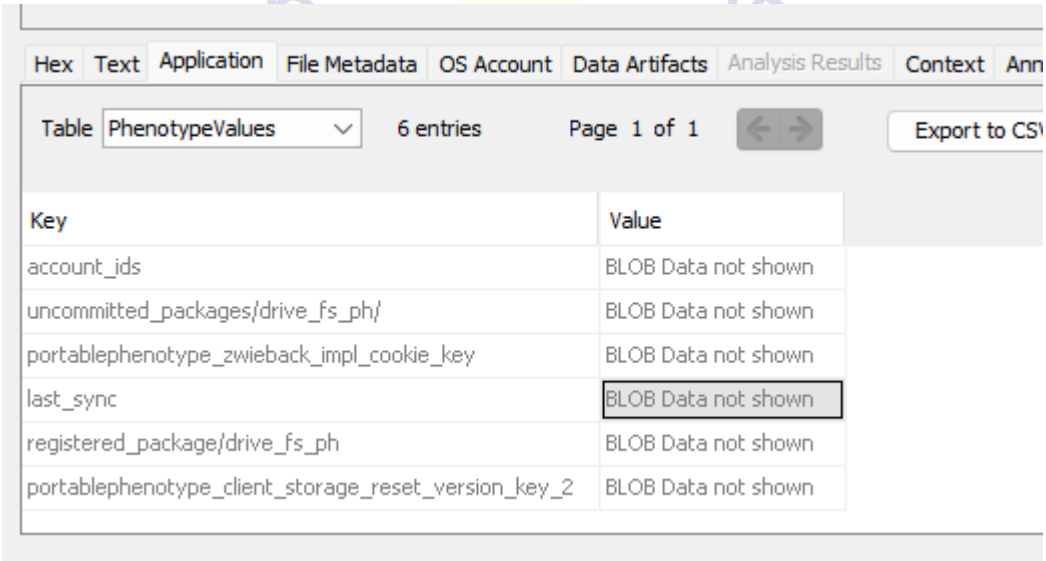


Figure 164 GDrive DB we can't find the Last sync

Crashpad		2023-05-09 17:32:54 IST	2023-05-09 17:32:54 IST
Logs		2023-06-23 14:49:41 IST	2023-06-23 14:49:41 IST
com.google.drive.nativeproxy.json	0	2023-06-23 14:49:40 IST	2023-06-23 14:49:40 IST
experiments.db	0	2023-06-23 14:49:40 IST	2023-06-23 14:49:40 IST
fallback-version	0	2023-05-09 17:35:28 IST	2023-05-09 17:35:28 IST
first-run-info	0	2023-05-09 17:24:42 IST	2023-05-09 17:24:42 IST
global_feature_config	0	2023-06-21 23:50:19 IST	2023-06-21 23:50:19 IST

Figure 165 Experiment. DB

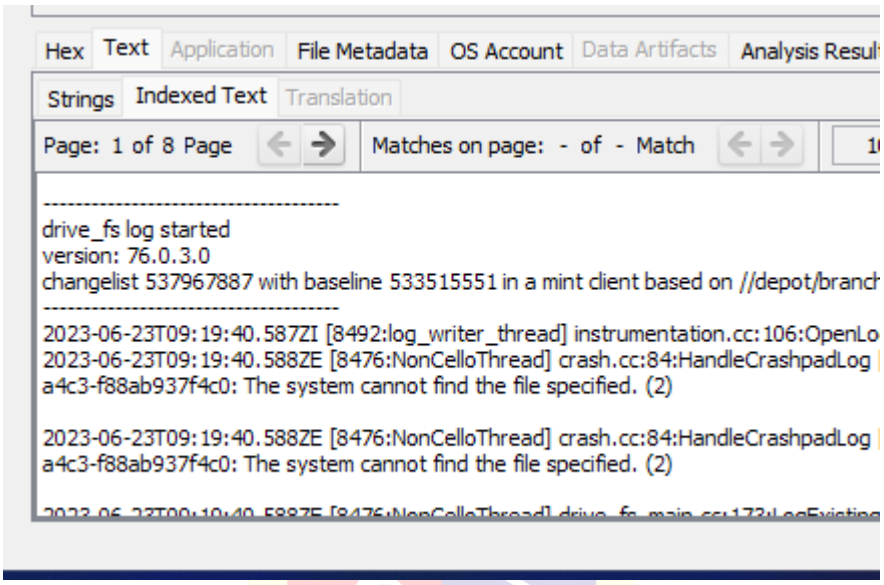


Figure 166 Version from Log

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

Table: media | 5 entries | Page 1 of 1 | Export to CSV

media_id	name	last_mou...	fs_type	device_t...	capacity	ignored
77aaa267-2...	USB_DEVICE_1683633282	C:\	4	2	64078475264	0
9776f337-1...	USB_DEVICE_1687433203	E:\	2	7	8192	0
5c3eecb1-1...	SANKLAP	E:\	4	7	61524127744	0
03bd1ed9-1...	Google Drive	G:\	10	2	5368709120	0
\\?\USB#AYB...	realme narzo 20		5	4	-1	0

Figure 167 GDrive stored USB entry in DB

metrics_store_sqlite.db-shm		2	2023-06-23 14:49:40 IST
metrics_store_sqlite.db-wal		0	2023-06-23 14:54:16 IST
pid.txt		0	2023-06-23 14:49:40 IST
root_preference_sqlite.db		0	2023-06-21 23:50:22 IST
root_preference_sqlite.db-shm		2	2023-06-23 14:49:40 IST
root_preference_sqlite.db-wal		0	2023-06-23 14:57:34 IST

Figure 168Root-Preference.DB

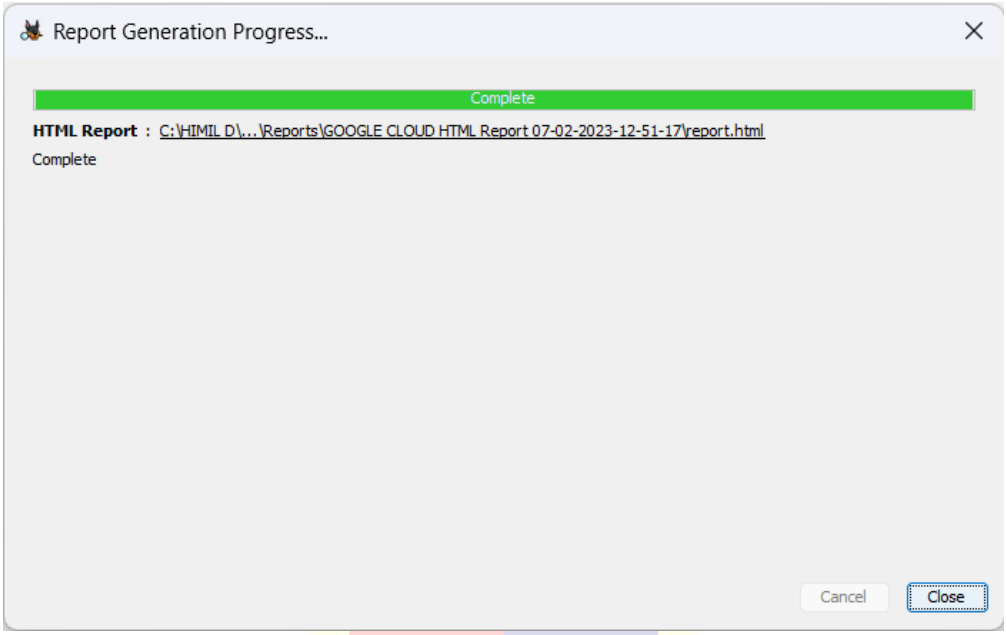


Figure 169 Google Drive report created successfully

15.7 Live browser artifact

	Hindsight Internet History Forensics (v2023.03)				
2	Type	Timestamp (US/Pacif	URL	Title / Name / Status	Data / Value / Path
3	url	2023-05-09 05:01:55.599	https://accounts.google.com/o/oauth2/auth?client_id=94731898980	Sign in - Google Accounts	
4	url	2023-05-09 05:01:55.599	https://accounts.google.com/v3/signin/identifier?opparams=%253F	Sign in - Google Accounts	
5	url	2023-05-09 05:01:56.302	https://accounts.google.com/v3/signin/identifier?opparams=%253F	Sign in - Google Accounts	
6	site setting (modif	2023-05-09 05:02:12.360	https://accounts.google.com:443,*	formfill_metadata [in Prefer	{'last_modified': '13328107332360141
7	url	2023-05-09 05:02:34.570	https://accounts.google.com/v3/signin/challenge/pwd?TL=AG7eRG	Sign in - Google Accounts	
8	autofill	2023-05-09 05:02:35.000		identifier	himil.dfis12211@nfsu.ac.in
9	url	2023-05-09 05:02:50.717	https://accounts.google.com/CheckCookie?continue=https://accoun	Redirecting	
10	url	2023-05-09 05:02:50.717	https://accounts.google.co.in/accounts/SetSID?ssdc=1&sidt=ALWU2	Redirecting	
11	url	2023-05-09 05:02:50.726	https://accounts.google.co.in/accounts/SetSID	Sign in - Google Accounts	
12	url	2023-05-09 05:02:50.999	https://accounts.google.com/signin/oauth/consent?authuser=0&pa	Sign in - Google Accounts	
13	url	2023-05-09 05:02:51.523	https://accounts.google.com/signin/oauth/firstparty/nativeapp?aut	Sign in - Google Accounts	
14	url	2023-05-09 05:02:53.618	http://127.0.0.1:49694/?state=v7WE7sJXi3mPKCSnlGqX&code=4/0Ab	127.0.0.1	
15	url	2023-05-09 05:04:33.318	http://127.0.0.1:49694/?state=v7WE7sJXi3mPKCSnlGqX&code=4/0Ab	127.0.0.1	
16	url	2023-05-09 05:04:33.471	https://accounts.google.com/o/oauth2/auth?client_id=94731898980	Sign in - Google Accounts	
17	url	2023-05-09 05:04:33.471	https://accounts.google.com/v3/signin/identifier?opparams=%253F	Sign in - Google Accounts	
18	url	2023-05-09 05:04:33.848	https://accounts.google.com/v3/signin/identifier?opparams=%253F	Sign in - Google Accounts	
19	autofill	2023-05-09 05:04:43.000		identifier	himil.dfis12211@nfsu.ac.in
20	url	2023-05-09 05:04:43.391	https://accounts.google.com/v3/signin/challenge/pwd?TL=AG7eRG	Sign in - Google Accounts	
21	url	2023-05-09 05:05:15.766	https://accounts.google.com/CheckCookie?continue=https://accoun	Redirecting	

Figure 170finding a history with auto fill data

Group	Setting Name	Value
Account Information		
	account_id	106807315777188389081
	email	himil.dfis12211@nfsu.ac.in
	full_name	Himil Prajapati
	gaia	106807315777188389081
	given_name	Himil
	hd	nfsu.ac.in
	is_supervised_child	-1

Figure 171email id used to search and profile name

0		clear_lso_data_enabled	<not present>
1	Per Host Zoom Levels		
2	Sync Settings		
3		last_poll_time	2023-06-24 09:02:13.662
4		last_synced_time	2023-07-02 16:52:20.125
5		cache_guid	uVaOzK1pyOxw1s9X+NYQqQ==
6		gaia_id	106807315777188389081
7		has_setup_completed	TRUE
8		requested	TRUE
9			
0			

Figure 172last poll time and sync time

93	cookie (created)	2023-05-11 01:02:16.407	.addthis.com/	ouid	<encrypted>
94	cookie (accessed)	2023-05-11 01:02:28.362	.lifewire.com/	_ga	<encrypted>
95	site setting (modif	2023-05-11 01:02:28.411	https://www.lifewire.com:443,*	media_engagement [in Prefe	{'expiration': '13336041748411149', 'last_modified': '13328
96	download	2023-05-16 11:05:03.461	https://dl.google.com/drive-file-stream/5-percent/GoogleDriveSetu	Complete - 100% [300444440	C:\Users\PC-04\Downloads\GoogleDriveSetup.exe
97	url	2023-05-16 21:54:59.355	https://drive.google.com/?authuser=0	Google Drive	

Figure 173Gdrive download successfully history

402	url	2023-05-17 11:02:53.007	https://www.google.com/search?q=goog+drive&oq=goog+drive&aq	goog drive - Google Search
403	url	2023-05-17 11:03:01.937	https://drive.google.com/drive/my-drive	My Drive - Google Drive
404	url	2023-05-17 11:03:01.937	https://accounts.google.com/ServiceLogin?service=wise&passive=1	Google Drive: Sign-in
405	url	2023-05-17 11:03:01.937	https://accounts.google.com/InteractiveLogin?continue=https://dri	Google Drive: Sign-in
406	url	2023-05-17 11:03:02.558	https://accounts.google.com/InteractiveLogin?continue=https://dri	Google Drive: Sign-in
407	url	2023-05-17 11:03:02.622	https://accounts.google.com/InteractiveLogin?continue=https%3A%	Google Drive: Sign-in
408	url	2023-05-17 11:03:02.626	https://accounts.google.com/InteractiveLogin/signinchooser?contin	Google Drive: Sign-in
409	url	2023-05-17 11:03:07.107	https://accounts.google.com/signin/v2/challenge/pwd?continue=ht	Google Drive: Sign-in

Figure 174GDrive sign in history

Findings

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

Challenges faced During Forensic Investigations Involving the Cloud

various kinds of issues that are posed to investigators in dealing with the cloud and found that investigating cloud services with the current methods was infeasible to be executed efficiently. The most prominent issues seemed to be the geographical, privacy and legal that are faced by the investigators.

With investigations involving the cloud, this can be even more challenging as it includes several thousand virtual machines multiple servers and a large amount of cloud users amongst which only one of them is relevant to the case. It would lead to an interruption of service for other users not involved in the case.

The computers are part of the cloud infrastructure and interoperate within the network without the user's knowledge. Further, the only identity management that is done with the lack of physical interaction is commonly usage of user ID's and password that can potentially be intercepted and abused by unauthorized users due to the open nature of the cloud. So, there is a huge void when it comes to tools that are available to support forensic investigators in dealing with cloud data centres. There is a lot of cross-platform development and a lack of standardization of infrastructure that makes it difficult to develop these tools for forensic data extraction.

Conclusions

The fast advancement and increase in quality of cloud technology is definitely pushing digital forensic to entire new level. The main goal of the project was to perform investigation in the cloud storage. How we can investigate and try to retrieve the files, which have been, have been deleted .we conclude that various antiques are deserted after the erasure and uninstalling of cloud storage The quantity of antiques that were influenced upon creation, cancellation, transferring and moving inside the application shifted.

Some virtualization security solutions are general-use and deliver specific security functions, like antivirus or data backups. Other solutions focus on cloud environments, while some emphasize securing virtual machines. Each of these types of security tools serve different purposes, so they are often used complimentarily. Business-critical applications or those with sensitive data may use many, or all, of these tools throughout the application's lifecycle.

- A lot of useful information can be found by analysing artifacts left by Cloud Storage clients
- Google Drive use SQLite databases to store information about files.
- Google Drive should have mechanism to encrypt database files.
- Google Drive mirror.log is useful to obtain information about deleted files.
- Ram analysis is useful to obtain information about client configuration. At somewhat id and password also
- Interesting information can be found by analysing traditional Windows artifacts.
- It is difficult to find the evidence for the deleted files, but with proper log analysis we get it
- OneDrive SyncDiagnostics.log File is Useful to obtain information about last sync.
- We’re Interesting information can be found by analysing traditional Windows artifacts (Browser, Thumbnails, PageFile.sys, etc.)
- It is Difficult To Find a password of OneDrive Account, Mega Pcloud Crypto password

Future Scopes

- We can expand the forensics From Windows Environment to the other Environment like Android, IOS
- We can expand this work to the direction of smart phone forensics.
- As the Cloud services are evolving day by day we can expand our works for other service provider as well like Drop Box, amazon, azure
- Develop Script Which Can Extract Drives Data from the Android mobiles and tablets without root permission.
- Find Out Database File of Drives
- We can make python script that will help us to find the details about deleted files using the log generated by the Drives
- Research different decrypt algorithm to decrypt the database.

SUGGESTIONS

Cloud computing defers in technologies, implementation, architecture. The forensic investigator must be familiar with the various cloud computing technologies and architecture in order to understand their operations. There should continuously research in cloud storage services in every increasing technology space.

References

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

Cloud computing - Wikipedia

Cloud Computing Architecture (tutorialspoint.com)

Personal Cloud Storage – Microsoft OneDrive

Cloud storage Full Seminar Report, abstract and Presentation download (123seminarsonly.com)

10 Advantages and Disadvantages of Cloud Storage - GeeksforGeeks

Cloud Computing Architecture and Components (guru99.com)

Architecture of Cloud Computing - GeeksforGeeks

Literature review:

Darren Quick, Ben Martini, Raymond Choo

Cloud Storage Forensics

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2365631 [2]

HyunjiChung, JungheumPark, SangjinLee, CheulhoonKang *Digital Forensics Investigation on cloud storage service,*

https://pdfs.semanticscholar.org/5908/41937a08afebca75e3fdc9bf6d9a60695194.pdf [1]

(Vikas Sihag, Himanshu Mishra's, Gaurav Choudhary, Nicola Dragoni

Cloud Storage Client Forensic: Analysis of MEGA Cloud

Cloud Storage Client Forensic: Analysis of MEGA Cloud (researchgate.net) [3]

Ming Sang Chan

Forensic Analysis of Google Drive on Windows

Title (ijiset.com) Forensic Analysis of Google Drive on Windows [5]

Ameer Pichan, Mihai Lazarescu, Sie Teng Soh

Cloud forensics: Technical challenges, solutions and comparative analysis

Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud, and pCloud - ScienceDirect (TF_Template_Word_Windows_2010 (arxiv.org)) [4]