CLOUD STORAGE FORENSIC ARTIFACTS: PCLOUD STORAGE CASE

NURSABRINA BINTI AZELI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[CLOUD STORAGE FORENSIC ARTIFACTS: PCLOUD STORAGE CASE]

[NURSABRINA BINTI AZELI]

This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Software Development)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

[CLOUD STORAGE FORENSIC ARTIFACTS: PCLOUD STORAGE CASE]

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : *sabrina* Date : 14/09/2023

(NURSABRINA BINTI AZELI)

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of [Computer Science (Software Development)] with Honours.

SUPERVISOR : _ Date : 23/09/2023

DR. ZAHEERA ZAINAL ABIDIN
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi (FTMK)
Universiti Teknikal Malaysia Melaka (UTeM)

DEDICATION

I dedicate this research study to my parents, whose unwavering love and support have been the foundation of my academic journey. Their sacrifices and encouragement have shaped me into the person I am today. This achievement is a testament to their unwavering dedication and the values they instilled in me.

To my supervisor, DR. Zaheera Zainal Abidin, thank you for your invaluable mentorship and guidance. Your expertise, passion for knowledge, and belief in my potential have inspired me to reach new heights.

Finally, I dedicate this research study to myself. This journey represents my determination, resilience, and commitment to personal and academic growth. It serves as a reminder of my ability to overcome obstacles and achieve my goals. I am proud of the dedication and effort I have invested.

To my parents, my lecturer, and myself, thank you for being instrumental in this research study. Your support, guidance, and belief in me have been the driving force behind my success.

ACKNOWLEDGEMENTS

I would like to extend my heartfelt gratitude to Universiti Teknikal Malaysia Melaka (UTeM) for granting us, undergraduate students from the Faculty of Information and Communication Technology (FICTS), a valuable opportunity to embark on our final year project journey.

Additionally, I would like to express my deepest appreciation to my supervisor, DR. Zaheera Zainal Abidin, for their unwavering support, invaluable guidance, and expert mentorship throughout the duration of this project. Their extensive knowledge, constructive feedback, and dedication to excellence have been instrumental in shaping the direction and quality of this research. I am truly grateful for their continuous encouragement and belief in my capabilities.

Furthermore, I am grateful to my fellow classmates and friends for their support, encouragement, and stimulating discussions that have enriched my understanding of the subject matter. Their camaraderie and shared experiences have made this research journey more enjoyable and memorable.

Lastly, I would like to express my deepest gratitude to my parents, Azeli Bin Abdullah and S.Rohaidah Binti Salleh, for their unwavering love, encouragement, and understanding throughout my academic pursuit. Their constant belief in my abilities and their sacrifices have been the driving force behind my accomplishments.

ABSTRACT

With the increasing prevalence of cloud storage services, the forensic analysis of cloud storage artifacts has become a critical area of research. This study focuses on the analysis of cloud storage forensic artifacts, specifically in the context of pCloud storage. The objective is to investigate the digital footprints left behind by user activities such as file uploads, deletions, and downloads within the pCloud environment. The research methodology involves evidence source identification and preservation, collection, examination and analysis, reporting and analysis of datasets within the pCloud storage platform to simulate user actions. The subsequent analysis aims to uncover and examine the traces and metadata associated with these actions. Various forensic techniques and tools will be employed to extract and interpret relevant information, including timestamps, file metadata, access logs, and user account details. The findings of this research study will contribute to the understanding of forensic artifacts specific to pCloud storage, shedding light on the digital evidence that can be extracted and analyzed. The insights gained will aid digital forensic investigators in identifying and reconstructing user activities within the pCloud environment. Additionally, the study will provide insights into the security and privacy implications associated with cloud storage services and contribute to the development of robust forensic methodologies for cloud storage analysis.

ABSTRAK

Dengan peningkatan kebolehcapaian perkhidmatan penyimpanan awan, analisis forensik terhadap artifak penyimpanan awan telah menjadi bidang penyelidikan yang penting. Kajian ini memberi tumpuan kepada analisis artifak forensik penyimpanan awan, khususnya dalam konteks penyimpanan pCloud. Objektif kajian adalah untuk menyiasat jejak digital yang ditinggalkan oleh aktiviti pengguna seperti muat naik, padam, dan muat turun fail dalam persekitaran pCloud. Metodologi penyelidikan melibatkan pengenalpastian dan pemeliharaan sumber bukti, pengumpulan, pemeriksaan dan analisis, pelaporan, dan analisis dataset dalam platform penyimpanan pCloud untuk mensimulasikan tindakan pengguna. Analisis seterusnya bertujuan untuk mengungkap dan mengkaji jejak dan metadata yang berkaitan dengan tindakan ini. Pelbagai teknik dan alat forensik akan digunakan untuk mengekstrak dan menafsirkan maklumat yang relevan, termasuk cap masa, metadata fail, log akses, dan butiran akaun pengguna. Hasil kajian ini akan menyumbang kepada pemahaman artifak forensik yang khusus kepada penyimpanan pCloud, menerangi bukti digital yang boleh diekstrak dan dianalisis. Wawasan yang diperoleh akan membantu penyiasat forensik digital dalam mengenal pasti dan membina semula aktiviti pengguna dalam persekitaran pCloud. Selain itu, kajian ini akan memberikan wawasan mengenai implikasi keselamatan dan privasi yang berkaitan dengan perkhidmatan penyimpanan awan dan menyumbang kepada pembangunan metodologi forensik yang kukuh untuk analisis penyimpanan awan.

TABLE OF CONTENT

List of Tables

LIST OF FIGURES

Chapter 1: Introduction

1.1 Introduction

Due to the benefits of cloud storage, in recent years, there has been a remarkable rise in the utilization of cloud storage. Based on the recent report publish by Acumen Research and Consulting (2023), "*As of 2021, over 80% of businesses use cloud storage solutions.*" Despite the widespread popularity and extensive use of cloud computing in comparison to traditional and local storage methods, there are still cloud users who are conscious of the security and privacy concerns associated with cloud storage services. Security experts have discovered solutions that can be considered to protect the stored data and protect the privacy of the cloud users (Mohtasebi, S. H., et al., 2017).

In this study research, cloud storage, pCloud is used as a case study to identify possible evidence data that may remain after the use of pCloud in computer system. pCloud users can store, sync, and share their files, as well as make backup from other cloud services such as Dropbox. pCloud offers encryption on the client side, ensuring that the data leaving the client's system is securely encrypted. In addition, pCloud holds certifications for Quality Management Systems (ISO 9001:2008) and Information Security Management Systems (ISO 27001:2013), demonstrating their commitment to maintaining high standards in both quality management and information security.In light of the growing popularity of PCloud and its positive reviews from cloud experts, this research will specifically concentrate on investigating potential privacy concerns associated with pCloud (Mohtasebi, S. H., et al., 2017) .

Table 1.1: Summary of pCloud (cloud storage service)

Features	**pCloud**
Size of storage	10 GB
Security	Uses TLS/SSL encryption, applied when information is transferred from your device to the PCloud servers
File versioning	Yes
Area of specialization	With pCloud your valuable files are accessible even offline

File size restriction	Unlimited
OS supported	Windows OS, Mac OSX, Android platform, iOS, and Linux

1.2 Problem Statement (PS)

In this research, a few factors are analyzed to do the analysis in the cloud storage service, pCloud.

Table 1.2: Problem statement

PS	Problem Statement
	Cloud storage service is a worldwide service that has been used by people around the world and companies due to the advantages. However, despite all the advantages given by the cloud storage service, there is a issue regarding the security and the privacy in cloud storage.

1.3 Research Questions (RQ)

This research focuses on three research questions, these research questions is a guideline to complete the analysis of the cloud storage.

Table 1.3: Research questions

PS	RQ	Research Questions
	RQ_1	What data (and the location of the data) can be found on Windows operating systems when using pCloud services?
	RQ_2	What data can be leaked while accessing the pCloud using Google Chrome browsers and desktop applications on Windows operating systems?
	RQ_3	How can analysis effectively have documented in a forensic report?

1.4 Research Objectives (RO)

Based on the problem statement and research questions, research objectives

Table 1.4: Research objectives

PS	RQ	RO	Research Objective
	RQ_1	RO_1	To study type of data in the PCloud storage.
	RQ_2	RO_2	To analyse data breach while accessing the PCloud using Google Chrome browsers and desktop applications on Windows operating systems.
	RQ_3	RO_3	To produce a forensic report.

1.5 Scope of research

The scope of this research will focus on the analysis of the pCloud application for digital forensics and refer to the objectives of this research. The scope of this research is:

- pCloud application provides a comprehensive understanding of the features, functionalities, and operational mechanisms it employs as a cloud storage service.
- Outline the precise goals of the digital forensic investigation conducted within the framework of the Cloud application, which may involve objectives such as data recovery, evidence collection, identification of user activities, or the detection of potential security breaches.
- Examine the storage mechanisms utilized by pCloud, which encompass file organization, metadata storage, and encryption methods. Assess the efficiency of encryption algorithms and analyze their implications for data forensics.
- Conduct an investigation into the logging and tracking capabilities of pCloud to assess the level of monitoring and reconstruction possible for user activities, including file uploads, downloads, and sharing, during a forensic analysis.

1.5.1 Research contribution (RC)

In research contribution, based on the research objectives concluded the contribution of the research study.

Table 1.5.1: Research Contribution

PS	RQ	RO	RC	Research Contribution
	RQ_1	RO_1	RC_1	Identification of data in pCloud.
	RQ_2	RO_2	RC_2	Analysis of data breach in pCloud in various browser.
	RQ_3	RO_3	RC_3	The forensic report.

1.6 Report Organization

In this research study report divided into seven chapter. Chapter one is explaining introduction of the research study, Chapter two reviewing literature review of this research, Chapter three, is purpose of the methodology used based on the research of the topic, Chapter four is the experimental setup to do analysis of the research, Chapter five is the implementing of the analysis of the research, Chapter six is the…and lastly Chapter seven.

- **Chapter One: Introduction**

This chapter elaborates in depth on the background of the chosen topic for this research study. The background of the research topic is to identify problem statement and research questions. Then, research objectives are achieved by fulfilling the problem statement and research questions.

- **Chapter Two: Literature Review**

A literature review in this research paper provides a concise summary and analysis relevant to the research topic. This chapter outlines and analyses previous works of research to analyse and justify solutions and methods used for the research study.

- **Chapter Three: Research Methodology**

Chapter three discusses the suitable research methodology to use in the research for a suitable guideline. A brief explanation of the methodology and how it works with the research study.

- **Chapter Four: Design and Implementation**

The experimental setup provides overview information on how the research was conducted. It includes a description of the procedures and tools used to conduct the research and analysis.

- **Chapter Five: Analysis and Findings**

  In this chapter, analysis and findings on the cloud storage using tools are started. Analysis will be done based on the objectives of this research to collect specific data needed.

- **Chapter Six: Conclusion**

  In chapter conclusion, project will be summarized and analyse the impact of this research towards forensic field.

1.7 Summary of Introduction

In summary, this research offers a comprehensive analysis of cloud storage from a digital forensic perspective. The primary aim of this study is to accomplish the research objectives and provide a systematic approach for digital analysts to analyze cloud storage. The current chapter presents the problem statement, research questions, research objectives, and research contributions. The subsequent chapter, the literature review, will provide a concise overview of existing research conducted by other scholars on digital forensic cloud storage. Through this review, a comparative analysis of frameworks will be conducted to identify the most appropriate framework for this research study.

Chapter 2: Literature Review

2.1 Introduction

This chapter goes through several research papers that are related to digital forensic investigation and analysis of cloud storage. Research papers included in this section contain different types of cloud storage used in digital forensic analysis to get remnants from cloud storage. This literature review explains in depth each topic involved in this research study: cloud computing, explaining how cyber criminals used cloud storage to commit crime, and pCloud (cloud storage used as a case study).

2.2 Cloud Storage

As data volumes continue to expand rapidly and organizations seek to ensure its long-term security, there is a growing necessity to integrate data management and utilization throughout its lifecycle. One emerging option is storing data on the internet, utilizing off-site storage services provided and maintained by third-party entities. This concept is illustrated in **Figure 2.2**. Cloud storage presents a substantial storage resource pool with three key characteristics: access through Web services APIs over an intermittent network connection, immediate availability of extensive storage capacities, and a pay-as-you-go model where users only pay for the storage they utilize. Additionally, cloud storage facilitates rapid scalability to accommodate evolving needs (Broberg, J., et. al., 2009).

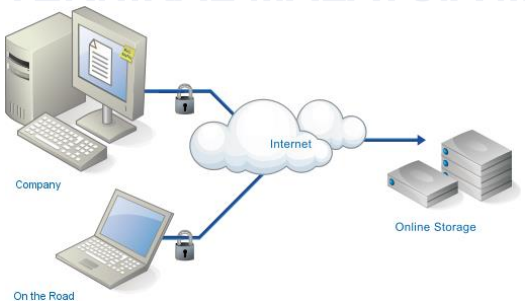


Figure 2.2: Simple cloud storage model

(Source: loretoweir.com)

2.2.1 Evolution of Cloud Storage

Cloud storage is a fundamental component of cloud computing, as illustrated in **Figure 2.2.1**, depicting its evolution from traditional network storage and hosted storage solutions. One of the significant advantages of cloud storage is the ability to access data from any location. Cloud storage providers offer a range of storage options, accommodating small

data volumes to even the entirety of an organization's data warehouse. Subscribers have the flexibility to pay the cloud storage provider based on their usage and the amount of data transferred to the cloud storage platform (Rajan, R.,A., et. al., 2012).

In cloud storage, the subscriber uploads their data to one of the data servers belonging to the cloud storage provider. This data copy is then replicated across multiple data servers within the provider's infrastructure, ensuring redundancy and availability. This redundancy measure guarantees the safety of the subscriber's data even in the event of any mishaps. Many systems employ servers with diverse power supplies to store the same data, further enhancing data protection (Rajan, R.,A., et. al., 2012).

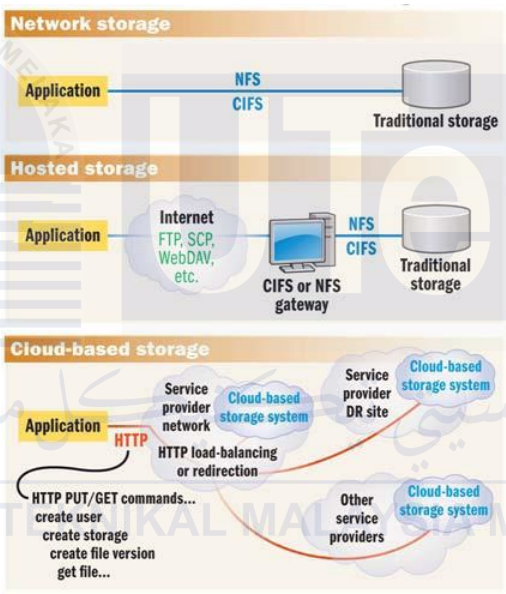


Figure 2.2.1: Evolution of cloud storage

(Source: researchgate.net)

2.2.2 Cloud Storage Reference Model

Cloud storage offers similar attributes to other cloud services, which contribute to its appeal. These include a pay-as-you-go model, the perception of infinite capacity (elasticity), and user-friendly management and usability. Hence, it is crucial for any cloud storage interface to incorporate these attributes, enabling support for various business scenarios and offerings, both in the present and for future requirements (Venugopal, S., 2006).

The model developed and published by the Storage Networking Industry Association (SNIA) demonstrates various types of cloud data storage interfaces capable of supporting both legacy and new applications. These interfaces enable on-demand storage provisioning

from a shared resource pool. Storage capacity is sourced from a pool of storage resources offered by storage services. Data services are applied to specific data elements based on the metadata of the data system. The metadata defines the data requirements for individual data elements or groups of data elements (containers) (Rajan, R.,A.,P., et. al., 2012).

As illustrated in **Figure 2.2.2**, the Cloud Data Management Interface (CDMI) serves as the functional interface enabling applications to perform operations like data creation, retrieval, update, and deletion within the cloud environment. Through this interface, clients can explore the capabilities of the cloud storage service and effectively manage containers along with the data stored within them. Furthermore, metadata can be assigned to containers and their associated data elements using this interface. The interface is designed to be compatible with the majority of existing cloud storage offerings, either through the implementation of an adapter for their proprietary interfaces or by directly integrating the CDMI interface. Existing client libraries, such as the extensible Access Method (XAM), can also be modified to support this interface, as depicted in Figure 2.2.2 (Rajan, R.,A.,P., et. al., 2012).

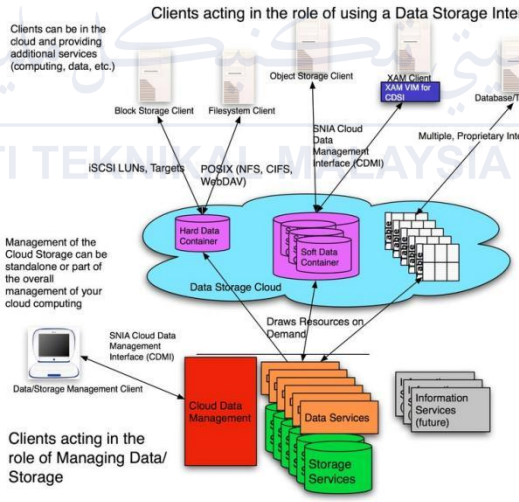


Figure 2.2.2: Cloud storage reference model

(Source: researchgate.net)

Administrative and management applications utilize the same interface to handle various tasks such as container management, account management, security access control, monitoring and billing information, and even accessing storage through other protocols. The interface ensures that the functionalities and features of the underlying storage and data services are transparent to clients, allowing them to comprehend the available offerings. Cloud offerings

that adhere to the standards may choose to offer a subset of the interface, as long as any limitations in capabilities are clearly communicated through the designated part of the interface (Rajan, R.,A.,P., et. al., 2012).

2.2.3 Cloud storage API

A Cloud Storage Application Programming Interface (API) enables users to access and utilize a cloud storage system. The predominant types of these APIs are REST (REpresentational State Transfer), although there are alternative options based on SOAP (Simple Object Access Protocol). These APIs facilitate the process of making service requests over the Internet. REST is widely acknowledged as a preferred approach for designing scalable APIs that emphasize quality (Vaquero, L. M., et. al., 2008).

One of the key advantages of REST is its "stateless" architecture, which means that all the necessary information to fulfill a request to the storage cloud is contained within the request itself. As a result, there is no need for an ongoing session between the requester and the storage cloud. This aspect is particularly significant due to the inherent latency of the Internet, which is characterized by unpredictable response times and generally slower speeds compared to local area networks. REST aligns well with the nature of the Internet and overcomes the limitations of traditional file storage access methods like NFS (Network File System) or CIFS (Common Internet File System), which are not suitable for efficient operation over the Internet due to latency issues (Vaquero, L. M., et. al., 2008).

Cloud storage primarily caters to storing files, often referred to as objects or unstructured data. These files encompass a wide range of formats such as pictures, spreadsheets, and documents, exhibiting significant variability and lacking a strict structure. On the other hand, there is another category of data known as block or structured data, which typically includes database data and feeds transactional systems that demand guaranteed or low-latency performance. Cloud storage is not designed for this particular use case (Rajan, R.,A.,P., et. al., 2012).

According to estimates by the Industrial Design Centre (IDC), approximately 70% of the globally stored machine data constitutes unstructured data, making it the fastest-growing data type. Cloud storage serves as a suitable solution for managing and accessing these unstructured files efficiently via the Internet. However, it's worth noting that accessing cloud storage is not limited to the public internet, as private networks or LANs can also provide

connectivity to a storage cloud using alternative approaches like NFS or CIFS. Nonetheless, the preferred and primary mode of access is through a REST API(Rajan, R.,A.,P., et. al., 2012).

REST APIs are independent of programming languages, allowing developers to easily utilize them regardless of the language they prefer. These APIs enable the manipulation of system resources through URLs, serving as a means for programming languages to interact with a storage cloud. It's important to note that an API itself is not a programming language, but rather a way to access and interact with a storage cloud using a programming language(Rajan, R.,A.,P., et. al., 2012).

REST APIs focus on altering the state of resources by working with representations of those resources. They are not solely about invoking functional web service methods. The primary distinctions among different Cloud Storage APIs lie in the URLs that define the resources and the format of the representations used. Various APIs are available, including Amazon S3 APIs, Eucalyptus APIs, Rackspace Cloud Files APIs, Mezeo APIs, Nivanix APIs, Simple Cloud API, as well as the standards proposed by the Storage Networking Industry Association (SNIA) Cloud Storage Technical Work Group, among others (Rajan, R.,A.,P., et. al., 2012).

2.2.4 Cloud storage challenge in data security issues.

Cloud storage is an important component of Infrastructure as a Service (IaaS). However, if the storage is not properly managed in the cloud environment, it can lead to significant consequences (Rehman, G-U., et al., 2020). The issues related to cloud storage can be divided into two main categories: data security and data management. This paper focuses on these categories and provides an overview of the challenges faced by cloud storage providers and users, along with potential solutions. Some points may overlap between the categories, but this differentiation helps in understanding the specific challenges (Jan, S.U. *et al.,* 2020).

2.2.4.1 Data Security Issues

Data security is a fundamental requirement for tenants, ensuring their rights are protected. A secure cloud storage service plays a pivotal role in attracting users to entrust their data to the cloud. Service providers in this domain strive to explore techniques that can effectively manage data access and enhance security measures. As data volumes continue to grow, so do the risks associated with data breaches and unauthorized interceptions. Cloud computing, offering a virtualized storage environment, places data control solely in the hands

of the service provider (Arockiam, L., et al., 2014). In such a scenario, users often raise pertinent questions regarding the exact location of their data, the implications of data deletion, and the permanence of data erasure.

The literature offers numerous solutions addressing data security in cloud environments. In reference, the authors have categorized these security measures into four layers, namely availability, authentication, confidentiality, and integrity. Their argument revolves around the notion that achieving confidentiality inherently ensures integrity (Arockiam, L., et al., 2014). However, this subsection focuses on a more comprehensive examination of the challenges associated with data security. A recent research investigation (Rehman, G-U., et al., 2020), which delved into data security and privacy in cloud storage, highlighted three key factors that stem from the inherent features of cloud computing, irrespective of the specific server technologies employed. These factors encompass outsourcing and multitenancy.

Data security is crucial for users who store their data in the cloud. Cloud storage providers aim to enhance security and control access to data. However, as data sizes increase, so does the risk of data attacks and interceptions. In a cloud environment, users have limited control over their data. This raises questions like the exact location of the data, what happens when data is deleted, and whether deleted data is truly erased **(**Jan, S.U. *et al.,* 2020).

The literature offers various solutions for cloud data security. One study categorized security solutions into availability, authentication, confidentiality, and integrity layers. It emphasized that achieving confidentiality ensures integrity. However, this subsection focuses on a more detailed exploration of data security issues (Rehman, G-U., et al., 2020). Another recent study highlighted three main reasons for data security concerns in cloud storage, independent of server technologies: outsourcing, multitenancy, and cloud computing features.

To address these challenges, Time Stamp Authority (TSA) and Public Key Infrastructure (PKI) technologies are introduced into cloud storage systems. They help with authentication, security, audit, and recording. User identification, time stamping, and user verification are crucial elements. PKI improves security, while authentication is handled through directory services. Time stamps provide audit and evidence with minimal overhead. TSA also optimizes data management in cloud storage (Kamara, S., et al., 2010).

In this approach, operations involve communication between the client and TSA server. No additional overhead is introduced as no certificate is used during communication. Operation

commands are converted to time stamps and sent to the TSA server for verification. Upon validation, a time stamp is issued and sent to the cloud for further operations. The cloud system stores time stamps and records of operations, such as queries, downloads, and uploads **(**Jan, S.U. *et al.,* 2020).

Data Security	Public Key Inscription	Low cost/system overhead
	Trusted Timestamps	Auditing, recording, data management
	Directory Services	Authentication, verification

Table 2.2.4.1: The basic approaches used in designing data security techniques (Jan, S.U. *et al.,* 2020)

In simpler terms, cloud data security is important, and solutions exist to address it. These solutions involve technologies like time stamps and authentication systems. They ensure the integrity and security of data stored in the cloud (Hittu, G., 2019).

2.2.4.1.1 Confidentiality issues

Cloud storage involves storing data on servers, which raises concerns about privacy. Confidentiality is essential for protecting sensitive information in the cloud. Encryption techniques are used to achieve confidentiality, but they can limit system operations and require encryption keys. Some systems combine encryption and obfuscation depending on the data type. A proposed solution is a proxy encryption system that consists of configuration, storage, transfer, and recovery stages (Arockiam, L., et al., 2014). It uses an RSA-based algorithm to generate keys and involves communication between the sender and recipient. Data privacy in cloud storage has important implications, such as the confidentiality of government, business, and personal information. The level of confidentiality depends on the cloud provider's privacy policies. Information disclosure can affect privacy rights and legal protection. Different storage locations may have different legal implications and consequences. Providers may be obligated to disclose or examine user records for legal reasons. Protecting user privacy and confidentiality in the cloud involves legal considerations (Ghani, A., et al., 2020).

2.2.4.1.2 Integrity Issues

Data integrity is crucial for any system, ensuring that the data is authentic and reliable. In a standalone system, integrity can be achieved through constraints and transactions in a single database. However, in distributed systems like the cloud, where data is stored across multiple sites, maintaining integrity becomes more complex. Transactions involving shared data across multiple sites must be carefully handled to avoid failures and allow different applications to participate in the overall transaction (Ghani, A., et al., 2020).

With the rise of Service-Oriented Architecture (SOA) and Cloud computing, data integrity issues become more significant. These environments involve a mix of local and Software as a Service (SaaS) applications, where functionality is exposed through APIs. Multi-tenancy is supported in SaaS applications hosted by third parties. Similarly, in SOA environments, applications use web services to expose their functionality. Managing transactions in such environments, especially with web services, presents challenges. The HTTP protocol does not inherently support guaranteed delivery or transactions, necessitating the implementation of transaction management at the API level (Ghani, A., et al., 2020).

2.2.4.1.3 Data Access Issues

Issues with accessing data in cloud storage often arise from security policies. Organizations may have specific policies that determine which employees can access certain data and which data is restricted. Cloud providers must adhere to these policies to prevent unauthorized access. The availability of services also requires verification of Service Level Agreements (SLAs) to ensure that user requirements are met (Samarat, P., et al., 2016).

In addressing data access problems, different access control methods are proposed in the literature. Role-Based Access Control (RBAC), User-Based Access Control (UBAC), and Attribute-Based Access Control (ABAC) are commonly discussed. UBAC is less suitable for cloud storage due to the overhead involved in managing access control lists (ACLs) for large datasets. RBAC assigns access based on user roles, making it suitable for enterprise-level organizations like hospitals. ABAC allows data owners to assign attributes and policies to users and data, granting access to users whose attributes align with specific policies. ABAC can be further divided into KP-ABE and CP-ABE, which differ in how keys and ciphertexts are linked (Ghani, A., et al., 2020).

However, attribute-based access control techniques can become computationally intensive, particularly for devices with limited resources like mobile devices. This complexity increases as the number of attributes used in decryption grows (Ghani, A., et al., 2020).

2.2.4.1.4 Authentication and Authorization Issues

Authentication is a crucial aspect of ensuring security in any system, acting as a gatekeeper that allows only trusted individuals to access cloud resources. It plays a key role in granting access to important information and must be robust to ensure only authenticated users can access it. By combining authentication with cryptography, not only data confidentiality but also integrity can be ensured. Implementing a sophisticated authentication mechanism can help address many security concerns (Ghani, A., et al., 2020).

Companies often use a Lightweight Directory Access Protocol (LDAP) server to store employee information. In small and medium-sized businesses, user management is commonly handled through Active Directory when adopting the Software as a Service (SaaS) model. This model allows software to be hosted outside the organization's firewall. To streamline user management, organizations may separate the user credential database from their internal IT infrastructure. This may involve keeping track of employees joining or leaving the organization and enabling or removing their accounts accordingly. Providers can delegate certain powers to the customer, such as allowing the customer's internal LDAP/AD server to handle user management. This helps reduce management overhead for customers using multiple SaaS products (Ghani, A., et al., 2020).

2.2.4.1.5 Data Breaches

In a cloud environment, multiple customers share the same infrastructure to store their data. This makes the cloud an attractive target for attackers because compromising the cloud means potential threats to the data of all users. External criminals pose the highest threat (73%) but with the least impact, compromising 30,000 records. On the other hand, insider threats have the lowest rating (18%) but the greatest impact, compromising 375,000 records. Partners fall in the middle with a rating of 73.39%, compromising 187,500 records (Ghani, A., et al., 2020).

Although SaaS providers offer better security compared to traditional methods, insider threats still exist. Employees of SaaS providers have access to a significant amount of information, which increases the risk of exposing customers' private information. To address

these concerns, SaaS providers should follow standards like PCI-DSS (Payment Card Industry-Data Security Standards) to ensure data security (Ghani, A., et al., 2020).

2.3 How cybercriminal use cloud storage in their crime.

Cloud computing accounts can be created, or existing accounts compromised for criminal purposes. New cloud computing accounts may be created with stolen credentials and credit card details, thereby reducing the cost to the offender(s), as well as anonymizing the offender and creating further difficulties in tracking down the source of the attack, particularly when jurisdictions are crossed. Accounts created or compromised in such a way can be controlled as part of a botnet (Hutchings, A., et al, 2015).

Botnet command-and-control servers can be used to launch DDoS attacks, conduct scams such as click fraud, and distribute spam. The processing power of botnets may also be used to conduct brute force attacks to overcome password restrictions. For example, there have been reports that hackers made use of a cloud computing server to launch attacks on Sony's payment platforms in April 2011. This attack resulted in the breach of the personal data (including name, date of birth, and email address) of 77 million users across the globe, and it was believed that the data of around 11 million credit cards may also have been leaked (Hong Kong Government News 2011). Cloud computing services may be used for the storage, distribution, and mining of criminal data such as stolen personal information or child exploitation material (Cloud Security Alliance 2010). Accounting systems run in the cloud may be attractive for money laundering and terrorism financing activities. The use of cloud computing to conduct illegal activities has had further negative consequences in relation to data access for other legitimate users of the cloud service provider when servers have been seized by a law enforcement agency. Not only may access be disrupted, but the law enforcement agency (international or domestic) may have access to that data in a multi-tenanted environment (Hutchings, A., et al, 2015).

2.3.1 Ransomware

Ransomware is one of the methods of exploitation by which attackers can steal and encrypt data on the victim's computer, demanding a ransom from the victim to restore the original files. Ransomware could be seen as pernicious program that exploits the victim's computer vulnerabilities to allow them to access and sneak onto the computer to encrypt the wanted files. Then the attacker will lock the files on the victim's computer; unless the victim pays the ransom, the files will be retrieved (Luo, X., & Liao, Q.,2007).

Personal devices such as laptops and desktops that most likely contain targeted files and personal information will be the target of the ransomware. However, corporate and company servers and data centres also become victims of ransomware. This is because the growing number of businesses is getting bigger, so it will be easier if the operations of the business are moved to the cloud in order to increase the availability and online presence and increase the business operations. However, cloud storage is still not immune to ransomware attacks (S Bhattacharya & C R S Kumar, 2017).

There are multiple ways for ransomware to be spread by the attacker, such as adware, malvertising, emails, zero-day exploits, and waterhole attacks. One of the most famous ways to source ransomware is through phishing emails. The attacker can easily use a trusted source and replicate the identity of the trusted source to lure the victim in. The victim can enter any credentials information, and it will be linked and captured at the malicious sites. Another method of ransomware attacks is malicious code infection through the downloading method. When victims visit the unsecured websites, malicious code is spread. This is because ransomware uses code insertion, so this method can be spread just by visiting a website (S Bhattcharya & C R S Kumar, 2017).

2.4 Technique(s) Used in Analysis of Cloud Storage

In the world of cloud storage, analysis is crucial for understanding and improving storage systems. As cloud storage becomes increasingly important in today's computing environments, it is necessary to explore the different techniques used for analyzing cloud storage.

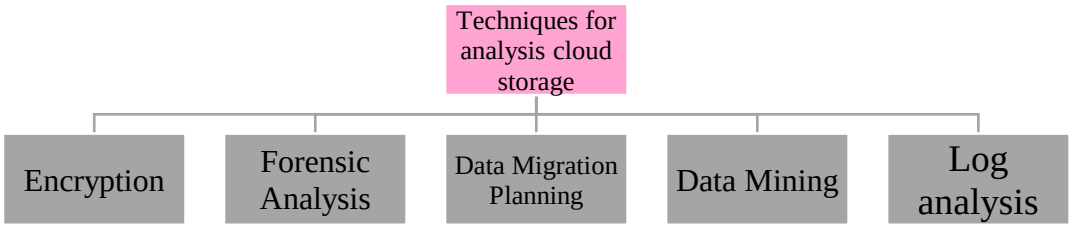


Figure 2.4: Technique(s) of analyse Cloud Storage

These techniques serve different purposes and provide valuable insights for the analysis process. Based on the **Figure 2.4** shows different techniques can be used in analysis of cloud storage.

Table 2.4 (1): Comparison of cloud storage analysis technique(s)

	Purpose and Focus	**Goals**	**Scope**	**Objective**	**Application**	**Outcome**
Encryption	Assess and analyze encryption mechanisms used in cloud storage.	Evaluate the strength and effectiveness of encryption measures.	Focuses on encryption algorithms, key management, and security protocols.	Identify vulnerabilities or weaknesses in encryption practices.	Assessing the security of data in transit and at rest.	Recommendations for enhancing encryption and data protection.
Forensic Analysis	Investigate digital artifacts and gather evidence related to security incidents or breaches.	Uncover evidence, reconstruct events, and determine the cause or origin of incidents.	Examines digital artifacts, data remnants, and system logs.	Gather evidence to support investigations and legal proceedings.	Investigating security breaches, unauthorized access, data loss, etc.	Identification of culprits, incident reconstruction, and legal proceedings if necessary.
Data Migration Planning	Plan and manage the migration of data between different storage systems or environments.	Ensure smooth and efficient migration of data while minimizing disruption and ensuring data integrity.	Involves planning and coordination of data migration processes, including data mapping and transfer protocols.	Ensure successful migration of data with minimal disruption and data loss.	Planning and executing data migration projects, such as cloud migration or system upgrades.	Successful migration of data with minimal disruption and data integrity ensured.
Data Mining	Extract valuable insights and patterns from data stored in	Discover hidden patterns, relationships, and trends in cloud	Analyzes large volumes of data to extract meaningful	Make informed decisions, predictions,	Optimizing resource allocation, identifying	Actionable knowledge and insights for decision-making,

	cloud storage.	storage data.	information and insights.	and optimizations based on data analysis.	trends, and making predictions based on cloud storage data.	prediction, and optimization.
Log Analysis	Analyze log files to extract information and identify patterns or anomalies for troubleshooting and security purposes.	Identify and analyze log entries to track system activities, detect security incidents, and investigate system issues.	Focuses on analyzing log files generated by various systems or applications for auditing, troubleshooting, and security analysis.	Extract valuable information from log files to improve system performance, detect anomalies, and enhance security measures.	Analyzing log files from various systems, including network devices, servers, and applications, for monitoring, troubleshooting, and security analysis.	Insights into system activities, identification of security incidents, and improved system performance through log analysis.

Based on **Table 2.4 (1)**, Forensic analysis is a crucial technique to use in this research study in cloud storage analysis as it allows for a comprehensive examination of digital artifacts, system logs, and data remnants. Through this analysis, a clear timeline of events can be established, enabling the identification and understanding of the nature and extent of the incident. **Table 2.4 (2)**, provide phase flow in the forensic analysis using the Martini and Choo framework.

By delving into the details of the incident, forensic analysis helps in understanding how the security breach or incident occurred, what actions were taken, and the potential impact on the cloud storage environment. This information is vital for incident response, risk assessment, and taking appropriate measures to prevent similar incidents in the future. Forensic analysis plays a significant role in uncovering crucial evidence, reconstructing events, and gaining a deeper understanding of security incidents in cloud storage systems.

Table 2.4 (2): Summary of phases forensic analysis on cloud storage with tools

Phase	Tools	Description
Evidence source identification and preservation		- In this phase, there is no tools used, as this phase is an identification phase and preserve the data.
Collection	NirSoft ChromeCacheView, Hex editor	- NirSoft ChromeCacheView viewing and extracting files from the cache of Google Chrome. - Hex editor, analyzing and interpreting raw data, file headers, or file system structures.

Examination and analysis	SQLite DB Browser, Hex editor	- SQLite DB Browser, explore and query databases containing metadata or user information. - Hex editor, analyzing and interpreting raw data, file headers, or file system structures.
Reporting and analysis	HashCalc	- used to generate hash values for evidence files to verify data integrity during analysis and to compare against known hash values to identify potentially malicious or tampered files.

2.5 Forensics Investigation Framework(s)

In this section, a comprehensive review is provided, drawing upon research in the fields of cloud and digital forensics. This review has been conducted after an extensive analysis of the existing literature. The scope of this work encompasses the methodologies and frameworks put forth by different researchers in the domains of digital and cloud forensics. It is important to note that most of the studies discovered predominantly concentrate on the investigative aspects and the methods employed for resolving cybercrime.

- **The Enhanced IDIP model**

  The Enhanced IDIP model distinguishes between primary and secondary crime scenes and represents the phases as iterative rather than linear. This model is based on the IDIP model but expands the deployment phase to include both physical and digital crime investigations and introduces a primary crime scene phase. It also introduces two additional phases: the trace back phase and the dynamite phase. In the trace back phase, the physical crime scene of operation is traced to identify the devices used in the act. The dynamite phase focuses on investigating the primary crime scene to collect and analyze relevant items for obtaining further evidence. Reconstruction occurs only after all investigations have been conducted (Baryamureeba, V., et al.,2004).

- **The Integrated Digital Investigation Process (IDIP)**

In 2003, the Integrated Digital Investigation Process (IDIP) model was introduced, drawing inspiration from the crime scene theory used in physical investigations. This model considers a computer itself as a crime scene and incorporates many similar phases found in previous models. It recognizes the importance of developing technical requirements for each phase and establishing the interaction between physical and digital investigations. The IDIP framework consists of 17 phases, organized into five groups: readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review. The readiness phase ensures that the necessary operations and infrastructure are fully capable of supporting an investigation. The deployment phase involves implementing mechanisms for detecting and confirming incidents. The physical crime scene investigation phase focuses on collecting and analyzing physical evidence, as well as reconstructing the actions that occurred during the incident. In contrast, the digital crime scene investigation phase involves identifying the electronic events that transpired on the system. Finally, the review phase entails evaluating the investigation to identify areas for improvement. A limitation of this model is that investigators cannot definitively determine whether a digital crime has occurred without conducting preliminary physical and digital investigations (Carrier, B., et al., 2003).

- **The Forensic Process**

In 2006, NIST proposed the Forensic Process, which comprises four phases: collection, examination, analysis, and reporting. According to this model, the forensic process involves converting media into evidence that can be used by law enforcement or for internal purposes within an organization. Initially, collected data undergo examination and extraction from the media, followed by transformation into a format compatible with forensic tools. Subsequently, the data is analyzed to derive meaningful information. Finally, during the reporting phase, the information is presented as evidence (Kent, K et al., 2006).

- **The Forensic Investigations Process**

The Forensic Investigations Process adapted for cloud environments is based on the original Forensic Process, but with modifications to align with the unique characteristics of cloud computing. Instead of the traditional stages, this process incorporates four distinct steps. Firstly, the purpose of the forensics requirement is determined. Secondly, the types of cloud services (SaaS, IaaS, and PaaS) are identified. Thirdly, the background technology used in the cloud environment is determined. Lastly, the various physical and logical locations involved in the investigation, including client side, server side, and developer side, are examined. It's important to note that this model does not include any subsequent actions after evidence collection (Guo, H., et al., 2012).

- **The Integrated Conceptual Digital Forensic Framework**

The Integrated Conceptual Digital Forensic Framework, introduced by Martini, differs from previous models in two key aspects. Firstly, the identification stage is considered as a distinct stage on its own, as it is essential to identify all potential evidence at the beginning of an investigation. Secondly, the framework proposes combining the preservation and collection stages into a single stage, as collected data should be preserved simultaneously. Therefore, the comparison framework should incorporate preservation within the collection stage. Additionally, the reporting and presentation stage is referred to as the presentation stage, encompassing all the reports that will be presented in a court of law and the closure of the case (Martini, B., et al., 2012).

2.5.1 Comparison of the Framework(s)

Table 2.5.1 (1) presents a comparison of the stages between the proposed models and the comparison framework. Based on the analysis in **Table 2.5.1 (1)**, most of the models align with the four stages of the comparison framework, with a few exceptions. Some stages or activities in the proposed models are merged into a single stage in the comparison framework. For instance, stages/activities like preparation, approach strategy, readiness and deployment, awareness, authorization, planning, notification, incident response, and survey are encompassed within the identification stage. The preservation-collection stage incorporates stages/activities such as acquisition, packaging, transportation, and storage. Examination analysis includes reconstruction, interpretation, and attribution. The presentation stage covers

reporting, decision-making, evidence return, closure, review, dissemination, and conclusion. Although documentation is associated with the preservation-collection stage, it runs parallel to the stages of the comparison framework, along with the chain of custody (Simou, S., et al., 2016).

Table 2.5.1 (1): Mapping stages/activities of forensic models with comparison framework

(Simou, S., et al., 2016).

Comparison Framework	Identification	Preservation-Collection	Examination-Analysis	Presentation
The Enhanced IDIP model, (*Baryamureeba, V., et al., 2004*)	Readiness - detection - notification - confirmation	Preservation - survey - documentation - search - collection	Examination - analysis - reconstruction	Submission - communication - review
The Integrated Digital Investigation Process (IDIP), (*Carrier, B., et al., 2003*)	Readiness - deployment	Preservation - survey - documentation - search - collection	Reconstruction	Presentation - review
The Forensic Process, (*Kent, K et al., 2006*)	X	Collection	Examination - analysis	Reporting
The Forensic Investigations Process, (*Guo, H., et al., 2012*)	Identification	Preservation - collection	X	X
The Integrated Conceptual Digital Forensic Framework (*Martini, B., et al., 2012*)	Identification	Preservation - collection	Examination - analysis	Reporting - presentation

To evaluate the complexity of the methodologies mentioned, complexity indicators have been defined based on the number of stages (S) and the number of phases per stage (P) in each methodology. The comparison framework proposed earlier is used for the analysis. Three complexity scales have been established: Low (L), Medium (M), and High (H). If the total number of stages and phases is less than three, the complexity is categorized as Low. If the total number of stages and phases is three or four, the complexity is classified as Medium. If the total number of stages and phases exceeds four, the complexity is deemed High. These indicators enable an accurate assessment of the complexity levels of the methodologies (Simou, S., et al., 2016).

Table 2.8 (2): Complexity of methodologies' stages

(Simou, S., et al., 2016).

Methadologies/ Models	Stages (S) and phases (p)	Identification	Preservation-collection	Examination-analysis	Presentation
The Enhanced IDIP model, (*Baryamureeba et al,2004*)	14	5(H)	5(H)	1(L)	3(M)
The Integrated Digital Investigation Process (IDIP), (*Carrier et al, 2003*)	17	4(M)	8(H)	2(L)	3(M)
The Forensic Process, (*Kent et al, 2006*)	4	-	1(L)	2(L)	1(L)
The Forensic Investigations Process, (*Guo et al, 2012*)	3	1(L)	2(L)	-	-
The Integrated Conceptual Digital Forensic					

Framework (*Martini et al., 2012*)	4	1(L)	1(L)	1(L)	1(L)

2.6 Related work

This section provides a concise overview of the current state-of-the-art in digital forensics investigation concerning cloud privacy. While limited research has been conducted on cloud storage privacy investigation compared to other areas of computer analysis, notable studies by Martini and Choo have made significant contributions. They conducted an analysis using ownCloud as a case study to identify valuable client and server-side artifacts for forensic practitioners engaged in cloud analysis (Dargahi, T., et al., 2017).

As the usage of cloud storage services continues to rise among individuals and organizations for storing and accessing various types of data, most investigations in the cloud context focus on analyzing the likelihood of privacy breaches in widely used cloud storage services. For example, Quick and Choo examined the processes of data gathering, browsing, and file synchronization in Dropbox, Microsoft SkyDrive, and Google Drive. Their research revealed remnants of data left behind when using SkyDrive on different devices, such as mobile phones and desktop computers. Similarly, they investigated the potential residual data on Windows 7 computers and Apple iPhone 3G devices when users utilize Dropbox or Google Drive for cloud storage (Dargahi, T., et al., 2017).

In a similar vein, Hale analyzed the digital artifacts that remain on a computer after accessing or manipulating Amazon Cloud Drive. Their findings included information like installation paths and upload/download operations. Chung et al. introduced a novel method to analyze digital artifacts found on accessible devices, including mobile phones (e.g., iPhone and Android smartphones) and desktop systems running different operating systems (e.g., Windows and Mac). They examined cloud services such as Amazon S3, Google Docs, Dropbox, and Evernote (Dargahi, T., et al., 2017).

In contrast to cloud storage services based on open-source platforms, Apple users have their own proprietary cloud storage solution called iCloud. Oestreicher focused specifically on investigating the iCloud service to identify any residual digital traces when using native Mac OS X during system synchronization with the cloud.

Table 2.6: Comparison of cloud storage (pCloud, DropBox, OneDrive and iCloud)

	pCloud	DropBox	OneDrive	iCloud
Free storage size	Up to 10 GB	2 GB	5 GB	5 GB
Security	Client-side encryption, TLS/SSL	Encryption at rest and in transit	Encryption at rest and in transit	Encryption at rest and in transit
File Versioning	Yes	Yes	Yes	Yes
Area of specialization	Secure file storage and sharing	General cloud storage	General cloud storage	Apple device integration
File Restricted	No specific file size restrictions	None	250 MB per file	No specific limit
OS Supported	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android	iOS, macOS, Windows

2.7 Critical Review

Choosing pCloud as a case study is justified for several reasons. Firstly, pCloud offers a comprehensive set of features and functionality, including cloud storage, file sharing, synchronization, and file versioning. Exploring these features can provide insights into the technical aspects and implementation strategies employed by pCloud.

Secondly, pCloud's emphasis on client-side encryption and security measures makes it an intriguing case study to understand data security in cloud storage systems. Analyzing its security protocols, encryption algorithms, and data protection mechanisms can contribute to best practices in this domain.

Additionally, pCloud's user-friendly interface and cross-platform compatibility make it a suitable subject for studying effective UI/UX strategies and addressing cross-platform development challenges. By focusing on pCloud, this case study can fill a research gap and contribute to the understanding of cloud storage systems and the evolving cloud storage industry, given pCloud's industry significance and sizable user base.

2.8 Summary of Literature Review

Overall, this literature review has provided a comprehensive understanding of the challenges, techniques, investigation frameworks, and related work in the field of forensic analysis in cloud storage. The findings from this chapter will serve as a foundation for the subsequent chapters, where we will delve into the methodology, experimentation, and analysis to gain deeper insights into the forensic analysis of cloud storage services, with a specific focus on pCloud as our case study.

3.0 Research Methodology

3.1 Introduction

In the context of a research study, milestones play an important role; serving as vital reference points for evaluating the overall progress of the study. Grasping the purpose and implementation of milestones is imperative for maintaining organizational efficiency, adhering to deadlines, and successfully achieving project objectives. Based on the literature review in Chapter 2, a research methodology is set based on the research study approach of the digital forensic analysis case study.

3.2 Methodology

In order to ensure the reliability of a digital forensic analysis, it is essential to adhere to a forensic investigation guideline. In this research study, the framework introduced by Martini and Choo will be use to conduct this forensic investigation. This framework comprises four crucial stages that are fundamental to the investigative process. The goal in using this framework was to do a complete and reliable digital forensic study.

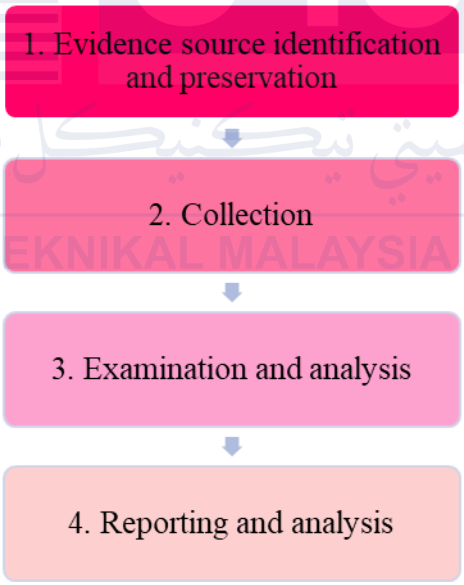


Figure 3.0: Martini and Choo Framework (Martini, B., & Choo, K.-K. R. 2012)

- **Evidence source identification and preservation:** it is necessary to gain a comprehensive understanding of the PCloud service and its features. Once a clear investigation scope has been established, the next step involves identifying the PCloud. Following that, the next task is to preserve the evidence in a manner consistent with forensic practices.
- **Collection:** The primary objective is to systematically gather relevant evidence from the pCloud platform. The process involve documenting pCloud details, and identifying

specific evidence sources aligned with the research objectives. Researchers employ suitable techniques, such as utilizing pCloud's features or third-party tools, to collect the identified evidence while maintaining data integrity. Comprehensive documentation of the collection procedures, including timestamps and any modifications, is crucial. Validation of evidence integrity is performed through hash value comparisons with the original sources. It is essential to securely store the collected evidence, adhering to industry best practices for preservation and security.

- **Analysis:** The focus is on examining and interpreting the collected evidence. This phase entails a thorough review and organization of the evidence to understand its content and context. Relevant information is extracted, aligned with the research objectives. Forensic analysis techniques are then applied to uncover hidden data, recover fragmented files, and identify patterns or correlations. The findings are interpreted, considering trends, anomalies, and patterns that support the research hypotheses. The analysis process is meticulously documented, capturing the techniques, tools, and observations made.
- **Reporting and presentation:** The focus is on documenting and presenting the findings in a clear and organized manner. After analyzing the collected evidence, a detailed report is created, outlining the research methodology, scope, and specific evidence sources. The report is structured logically, with sections for objectives, methodology, analysis, and findings. Visual aids, such as graphs or tables, may be included to enhance understanding. The findings are interpreted, explained, and related to the research objectives, highlighting their significance and potential implications. Additionally, visual presentations are prepared to present the research findings effectively.

3.3 Milestones

Table 3.3 (1): PSM 1 Milestones

WEEK	ACTIVITY	NOTES
W1 (20/03→24/03)	• Choosing an appropriate project topic and potential Supervisor. • Proposal PSM: Discussion with Supervisor. • Proposal assessment and verification.	• Title is chosen. • Proposal Form taken from Ulearn. • Proposal Form – email PIC (Dr. Fadzilah Othman)
W2 (27/03→31/03)	• List of students with project title versus supervisor and evaluator. • Proposal correction/improvement. • Proposal approval and submission.	• Email Committee for proposal approval. • Upload approved proposal at Ulearn.
W3 (03/04→07/04)	Chapter 1 • Meeting 2	
W4 (10/04→14/04)	Chapter 1 • Report Writing Progress 1	• Log progress – ePSM. • Deliverable – Chapter 1 – ePSM.
W5 (17/04→21/04)	Chapter 2	
W6 (24/04→28/04)	**MID-SEMESTER BREAK**	
W7 (01/05→05/05)	Chapter 2 • Report Writing Progress	• Log progress – ePSM. • Deliverable – Chapter 2 – ePSM.

	• Project Progress 1	• Progress Presentation 1 (KP1)
W8 (08/05→12/05)	Chapter 3	
W9 (15/05→19/05)	Chapter 3 • Report Writing Progress	• Log progress – ePSM • Deliverable – Chapter 2 – ePSM
W10 (22/05→26/05)	Chapter 4 • Project Progress 2 • Meeting with supervisor	• Log progress – ePSM. • Progress Presentation 2 (KP2)
W11 (29/05→02/06)	Chapter 4 • Report Writing Progress 2	• Log progress – ePSM Deliverable – Chapter 2 – ePSM
W12 & W13 (05/06→16/06)	• PSM1 Draft Report preparation	
W14 (19/06→23/06)	• PSM1 Draft Report submission to SV & Evaluator • Report Evaluation	• Log Progress – ePSM • Deliverable – Complete PSM1 Draft Report – ePSM
W15 (26/06→30/06)	• PSM 1 Demo and Report Presentation to Supervisor & Evaluator • Presentation Skill • Submission of PSM 1 documents to PSM supervisor, evaluator and committee in ePSM	• Log Record – ePSM • Submission of logbook in ePSM • Submission of Project Report PSM 1 to ePSM.

Table 3.3 (2): PSM 2 Milestones

WEEK	ACTIVITY	NOTE / ACTION
W1 (31/07→04/08)	Chapter 4 • Report Writing Progress	• PSM 1 correction and PSM 2 planning discussed with the supervisor.
W2 (07/08→11/08)	Chapter 5 • Analysis is started • Report Writing Progress	• Log Progress on ePSM. • Progress Presentation 1 (KP1). • Supervisor evaluate on ePSM.
W3 (12/08→18/08)	Chapter 5 • Analysis is started • Report Writing Progress	• Student working on Chapter 5. • Log Progress on ePSM. • Supervisor evaluate on ePSM.
W4 (21/08→25/08)	Chapter 5 • Analysis is started. • Report Writing Progress	• Student working on Chapter 6. • Log Progress on ePSM. • Progress Presentation 1 (KP2). • Supervisor evaluate on ePSM.

W5 (28/08→01/09)	Chapter 5 • Report Writing Progress	• Log Progress on ePSM. • Supervisor evaluate on ePSM. • Student working on Chapter 5.
W6 (04/09→08/09)	Chapter 6 • Report Writing Progress • PSM2 Draft Report preparation • PSM2 Draft Report submission to SV & Evaluator	• Log Progress on ePSM. • Deliverable of draft report to SV through email. • Supervisor evaluate on ePSM.

W6 (11/09→04/09) FINAL PRESENTATION	Report Evaluation DEMONSTRATION Supervisor DEMONSTRATION Evaluator English Proficiency [PRJ-7] Presentation Skill [PRJ-8]	• Log Progress on ePSM. • SV and EV evaluate on ePSM.
W6 (18/09→22/09) FINAL EXAMINATION WEEKS	• Correction on the draft report based on the Supervisor and Evaluator's comments during the final presentation session. • Do an online EoS Survey form. • Complete of overall marks to Committee • Submission of the final complete report, which is the updated & corrected PSM2 report	• Deliverable of EoS Survey, Online Form. • SV, EV and Committee Overall Evaluation PSM2 on ePSM • Deliverable the complete Final PSM Report on ULearn.
W9 (25/09→29/09) INTER-SEMESTER	• Submission of the final complete report, which is the updated &	• Deliverable the complete Final PSM Report,

BREAK	corrected PSM2 report and Plagiarism Report etc. onto the OneDrive	Plagiarism Report.

3.4 Gantt Chart

Table 3.4 (1): PSM 1 Gantt Chart

	Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Progress																
FYP Proposal																
Project Progress 1																
Report Writing Progress 1																
Project Progress 2																
Report Writing Progress 2																
Report Evaluation																
Demonstration																
Presentation																

Table 3.4 (2): PSM 2 Gantt Chart

Progress	Week	1	2	3	4	5	6	7	8	9
Project Progress 1										
Project Progress 2										
Report Writing Progress										
Report Evaluation										
Demonstration										
Presentation										
Submission Report										

3.5 Summary of Methodology

In conclusion, this research methodology contains components that outline the framework and procedures used to conduct the research study. Beside explaining the dataset used in the research study, milestones of this research, and a gantt chart for this research study.

Chapter 4: Design and Implementation

4.1 Introduction

In this chapter, design is approached for conducting forensic analysis of cloud storage systems. Four main components are encompassed in this chapter: proposed design, topology, software and hardware, and experimental setup. All these elements are taken into consideration based on the previous chapter.

4.2 Proposed Design

To enhance the methodology originally proposed by Martini and Choo, this study incorporates the utilization of keyword search as a fundamental technique. Keyword search methodologies entail the systematic examination for particular words or phrases, herein referred to as "keywords," within a given dataset or document repository with the primary objective of pinpointing pertinent information. In the domain of forensic cloud storage analysis, the keyword search technique is strategically employed to discern and extract digital artifacts or evidential elements that manifest specific words, phrases, or patterns of significance and relevance to the investigative context.

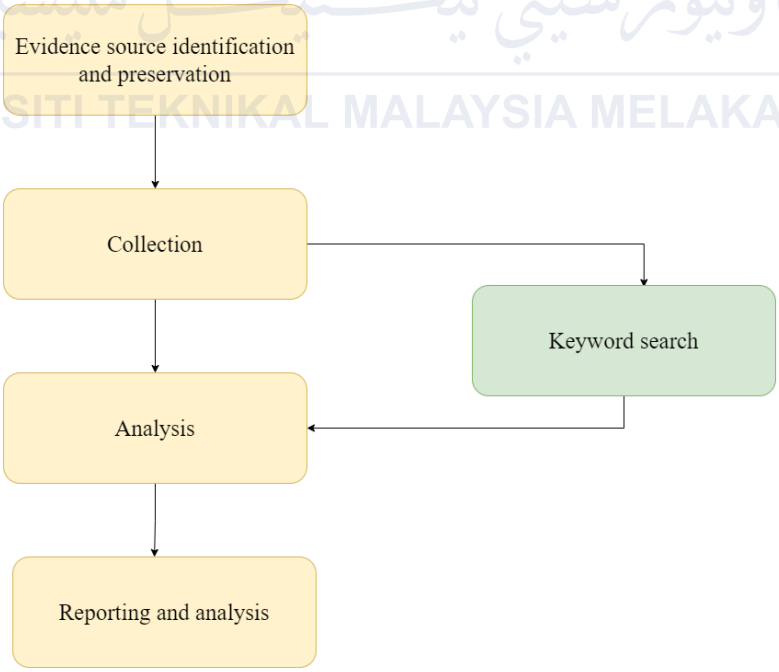


Figure 4.2: Framework of proposed design.

Based on the framework above (**Figure 4.2**) keyword search technique is put after collection phase. Collection data phase is a process require analyst to collect all data related to the case, with the keyword search technique, the analysis is done by searching a keyword to find a relevant data or artifacts left.

The keyword search phase employs a filtration technique, utilizing a string comparison mechanism. Analysts input a keyword relevant to the case, and the data is subsequently filtered through a string comparison method. The analysis then proceeds in both forward and backward directions. This process unfolds as follows:

1. Insert a collected data (e.g.: virtual memory file) into a chosen tools (e.g.: HXD editor), all the data showed on the layout.
2. By using search feature in the tools, forensic analyst starts identifying keyword that are relevant to the case or investigation, the process start with the first element on the right upper most, then analyst need to read an compare the data find simultaneously until the end of the update.
3. When a keyword match is found, the relevant data or artifact is flagged or extracted for further analysis.
4. If the keyword used is not giving any right evidence, then the searching process will be end and need to re-start the same process by using different keyword.

Keyword search is a valuable technique in forensic analysis as it allows investigators to quickly pinpoint potentially relevant information within a large dataset. However, it's essential to use appropriate search terms and carefully interpret the results to ensure the accuracy and relevance of the findings. Additionally, modern forensic tools may also offer more advanced search capabilities, such as regular expressions or fuzzy matching, to improve the effectiveness of keyword searches.

4.3 Topology

Figure 4.3 shows a topology for this research study. The diagram illustrates the topology of 6 VMs installed in one host machine, and it act as client. Each VM has it own task and each VM will make request connection to pCloud storage through Internet.

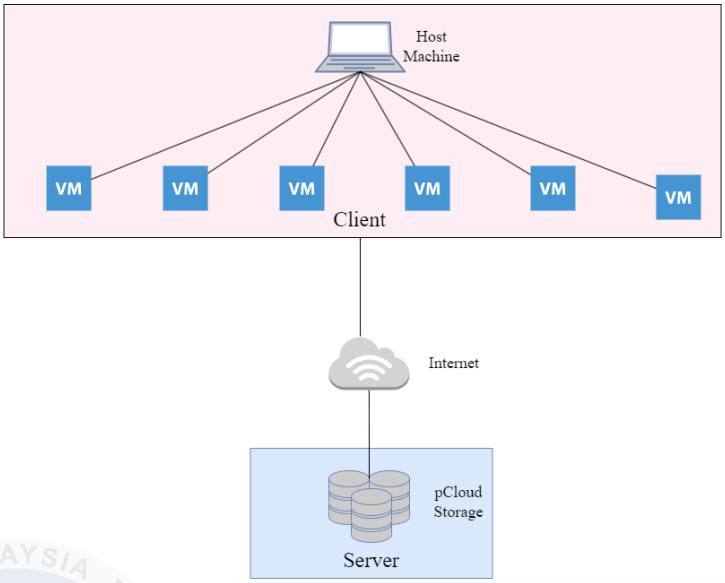


Figure 4.3: Topology of Experiment Setup

4.4 Software and Hardware

The section on software and hardware gives a clear picture of the technical parts involved in the research study. It focuses on the software programs and tools as well as the physical devices used in the study. This chapter helps you understand how the software and hardware choices are important for carrying out the study effectively and achieving the desired results.

4.4.1 Windows 10

Windows 10 is an operating system developed by Microsoft Corporation. It is running on the latest building known as 1709 (10.0.16299.125). Windows 10 offers features like Cortana, the Windows Store, Xbox integration, a start menu, and search tools. Windows 10 brings many new features compared to previous versions of Windows.

In this research study, we propose to utilize the Windows 10 operating system. Windows 10 is currently one of the most widely adopted versions of Windows, offering a diverse range of features and extensive usage. It incorporates various program s and mechanisms for effectively managing computer hardware and software (Ahmed, A. A., 2016). Presently, Windows 10 is known for its robust security measures, which present challenges in the field of digital forensics (Darsana, M. S., 2018).

4.4.2 VMware Workstation Pro

VMware Workstation Pro is a hypervisor that enables users to run multiple operating systems within virtual machines. Using a virtual machine offers several advantages compared to a native installation. One key advantage is the ability to run multiple operating systems simultaneously, providing added flexibility. Virtual machines also facilitate easy installation, re-installation, backup, and movement of guest operating systems, along with efficient allocation of system resources (Hintea, D., et al., 2017).

Another notable feature of VMware Workstation Pro is the capability to create snapshots. Snapshots allow users to save a stable state of the guest operating system on disk, enabling quick restoration of the virtual machine without the need for rebooting. Snapshots also offer the option to roll back to previously saved states, which is helpful for comparing any changes introduced by software installations or other actions within the operating system (Hintea, D., et al., 2017).

4.4.3 HashCalc

HashCalc is a software program developed by SlavaSoft. It serves as a free calculator for computing various types of hashes, checksums, and HMACs for files, text, and hexadecimal strings. The program supports popular algorithms such as MD2, MD4, MD5, SHA1, and SHA2 (including SHA256, SHA384, and SHA512). It offers three input data formats: file, text string, and hexadecimal string. HashCalc is known for its speed, user-friendly interface, and easy installation process. It can handle large files and supports drag-and-drop functionality for convenient use. HashCalc is particularly useful for verifying the integrity of files during FTP and other download/upload transfers. It allows users to compare different types of files, including music, audio, video, images, documents, and more. It is also capable of verifying CD and hard drive files, making it a valuable utility for checking the integrity of downloads, such as .mp3, .mpeg, .mpg, .avi, .vcd, .iso, .zip, .gif, .jpg, .doc, and other files.

4.4.4 Process Monitor

Process Monitor is an advanced monitoring tool designed for Windows operating systems. It was developed by Mark Russinovich and released as part of the TechNet Sysinternals Suite. The tool provides real-time visibility into file system activity, Registry modifications, and process actions. With Process Monitor, users can track attempts to read and write registry keys as well as file system operations. It offers filtering capabilities to

focus on specific keys, processes, process IDs, and values. In the context of investigations, Process Monitor is used to observe and analyze the changes made to the file system or registry by a particular action or application (Hintea, D., et al., 2017).

4.4.5 SQLite DB Browser

DB Browser for SQLite (DB4S) is a user-friendly and free software tool that aids forensic analysts in examining, modifying, and understanding data within SQLite databases. It simplifies the process of working with digital evidence by providing an intuitive interface, similar to a spreadsheet, which allows users to explore database content, make necessary changes, create reports, and analyze data relationships. This tool proves particularly valuable in forensic investigations where analysts need to extract and manipulate information from SQLite databases without requiring extensive database expertise.

4.4.6 Regshot

RegShot is a software tool used for taking snapshots of a Windows system's registry, allowing users to compare the state of the registry before and after making changes. It's commonly used in IT and troubleshooting tasks, as well as in system administration and software development, to track and analyze modifications made to the Windows registry. By providing a detailed record of registry changes, RegShot helps users diagnose problems, assess the impact of software installations or system modifications, and troubleshoot issues more effectively. It's a valuable tool for understanding how changes to the Windows registry can affect system behavior.

4.4.7 Hex Editor

A hex editor is a specialized software tool used for viewing and editing binary data at the hexadecimal level. It displays the contents of a file or storage device in a hexadecimal format, allowing users to examine and modify the individual bytes and data structures within the file. Hex editors are commonly used in various applications, including computer forensics, low-level programming, reverse engineering, and debugging, where a detailed understanding and manipulation of binary data are required. Users can typically view and edit the hexadecimal values, ASCII characters, and raw binary data, making it a versatile tool for working with files at a low-level, providing insights into file structures and facilitating data recovery and analysis.

4.4.8 Nirsoft Chromecacheview

NirSoft ChromeCacheView is a software utility developed by NirSoft, a well-known provider of small, specialized, and free system and network tools. ChromeCacheView is

specifically designed to extract and display the contents of Google Chrome's cache. Google Chrome stores cached copies of web pages, images, and other files locally on a user's computer to improve web page loading times and user experience. ChromeCacheView allows users to access and view these cached files, which can be useful for various purposes, including digital forensics, troubleshooting web-related issues, and recovering lost or accidentally deleted files from the cache. It provides details about cached files, such as their URL, file size, content type, and last accessed time, making it a handy tool for investigating web browsing activities or recovering specific files from the browser cache.

4.4.9 ExifTool

ExifTool is a powerful and versatile command-line software tool that allows users to read, write, and manipulate metadata (Exchangeable Image File Format or EXIF data) within digital media files, including images, audio files, and videos. It provides detailed information about the file's metadata, such as date and time, camera settings, geolocation, and more. ExifTool is widely used by photographers, digital forensics professionals, and anyone who needs to access or modify metadata in digital files. It supports a wide range of file formats and provides extensive capabilities for extracting, editing, and preserving metadata, making it an essential tool for managing and analyzing digital media files.

4.5 Experimental Setup

The experiment is conducted in a *64-bit Windows 10* operating system with a single browser, Google Chrome. The Digital Forensic Research Workshop Challenge dataset (DFRWS2) is used in the experiments. The dataset was downloaded on June 13, 2023, and its integrity is ensured by evaluating the hash using HashCalc. The primary folder within the dataset is named "test_01" and contains ten directories: "au," "b," "img," "js," "ml," "msx," "pdf," "txt," "vid," and "z.". Files in this folder will be used in the operation such upload, download, and delete.

4.5.1 Windows

To examine remnants of pCloud on a Windows operating system, two distinct research directions were pursued:

i. analysis based on Windows web browsers, and

ii. analysis based on Windows applications.

For the web browser-based investigation, *Google Chrome* was installed on four virtual machines (VMs). Each VM was assigned specific tasks related to the web browser. **Figure 4.5.1 (1)** illustrates the tasks performed on the Windows VM using the web browser. Subsequently, the VM was cloned to four other machines to carry out tasks such as uploading, downloading, opening, and deleting.

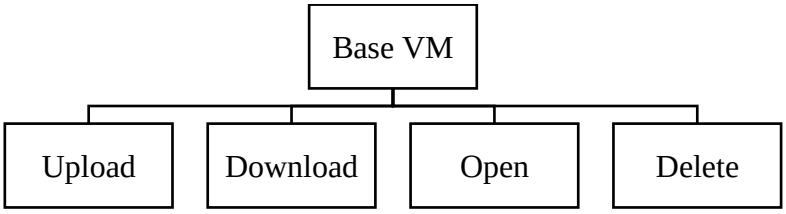


Figure 4.5.1 (1) : Windows browser-based VMs

Since the experiment focused on browser-based activities, there was no need to install pCloud. Instead, the experiment involved direct interaction with pCloud within the web browser. All folders and files from the DFRWS dataset were used for each task. For instance, all the files were uploaded during the upload task and subsequently downloaded during the download task. Additionally, network traffic was captured during all the tasks. The cache and history folders of web browsers contain important recoverable artifacts. Therefore, after conducting the upload, download, open, and delete operations using the dataset, the cache was analyzed.

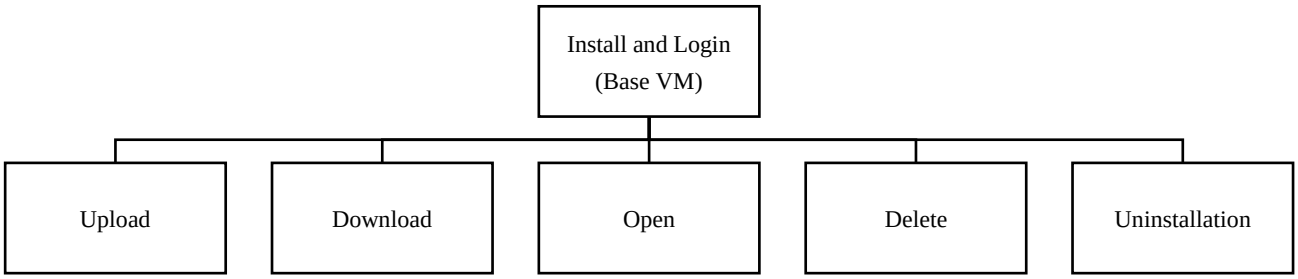


Figure 4.5.1 (2): Tasks performed on Windows app-based

For the Windows app-based investigation, Windows 10 with pCloud drive 2.0 was utilized. Six distinct tasks were executed, as depicted in **Figure 4.5.1 (2)**.

4.6 Summary of design and implementation

To sum up, the design and implementation chapter lays a strong groundwork for the forensic analysis of cloud storage in this study. It highlights the importance of the network

structure (topology), software and hardware choices, and the setup used for conducting experiments. These elements play a crucial role in ensuring that the results obtained from the study are trustworthy and meaningful. Paying close attention to these components is essential for successfully carrying out forensic analysis and obtaining valuable insights into the security of cloud storage.

Chapter 5: Analysis and Findings

5.1 Web browser-based

In the context of browser-based experiments, a rigorous analysis is conducted on pCloud using Google Chrome. These experiments involve the establishment of separate base virtual machines (VMs) to ensure the integrity of the testing environment, thereby mitigating the influence of any extraneous background variables. The experimental procedures encompass user login, file uploads, downloads, and file deletion processes.

5.1.1 Login

Chromecacheview, email and userid of user was exposed and cached in chrome browser via URL (https://eapi.pcloud.com/user/preparelogin?email=pcloudfp%40gmail.com&language=en&os=4). This remnant can help analyse to look for further information tied with the email and user id.

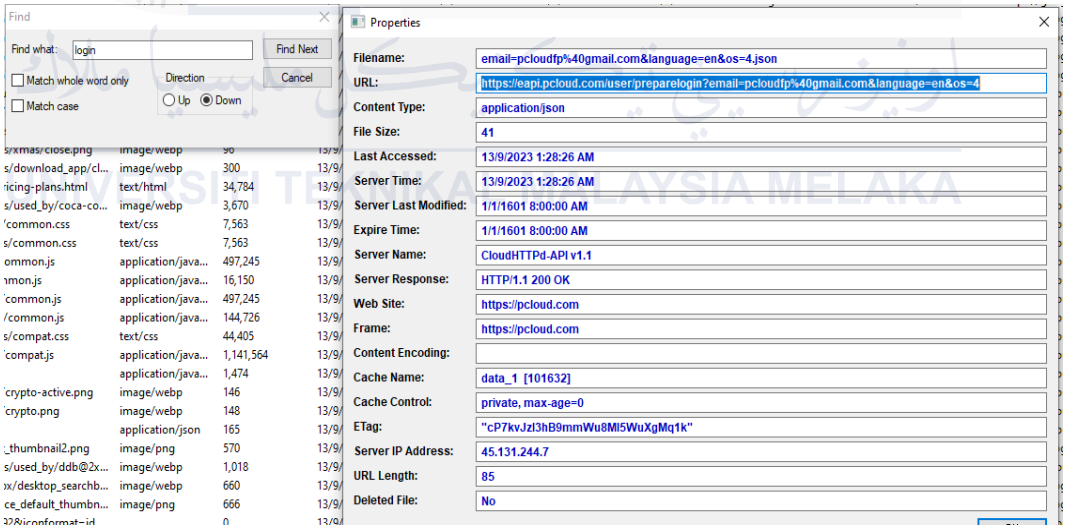


Figure 5.1.1 (1): email cached in chrome.

Livememory, several artifacts such as email, user id, email passwords, and cookie are found in the live memory. However, the user id was only found in the process dump file.

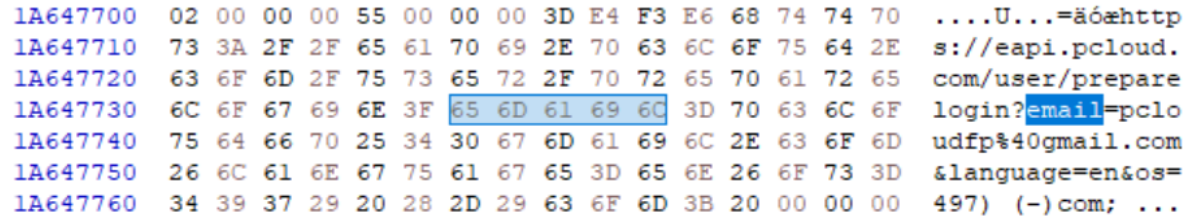


Figure 5.1.1 (2): email found in memory.

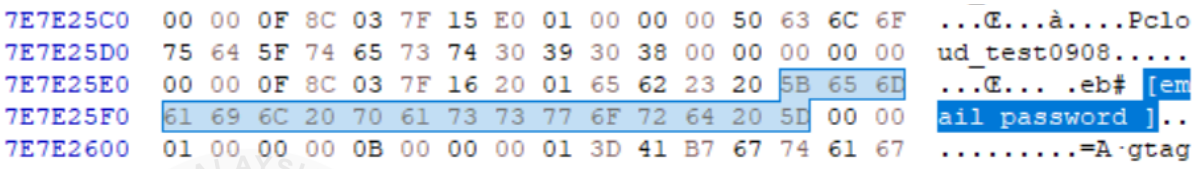


Figure 5.1.1 (3): password found in memory.

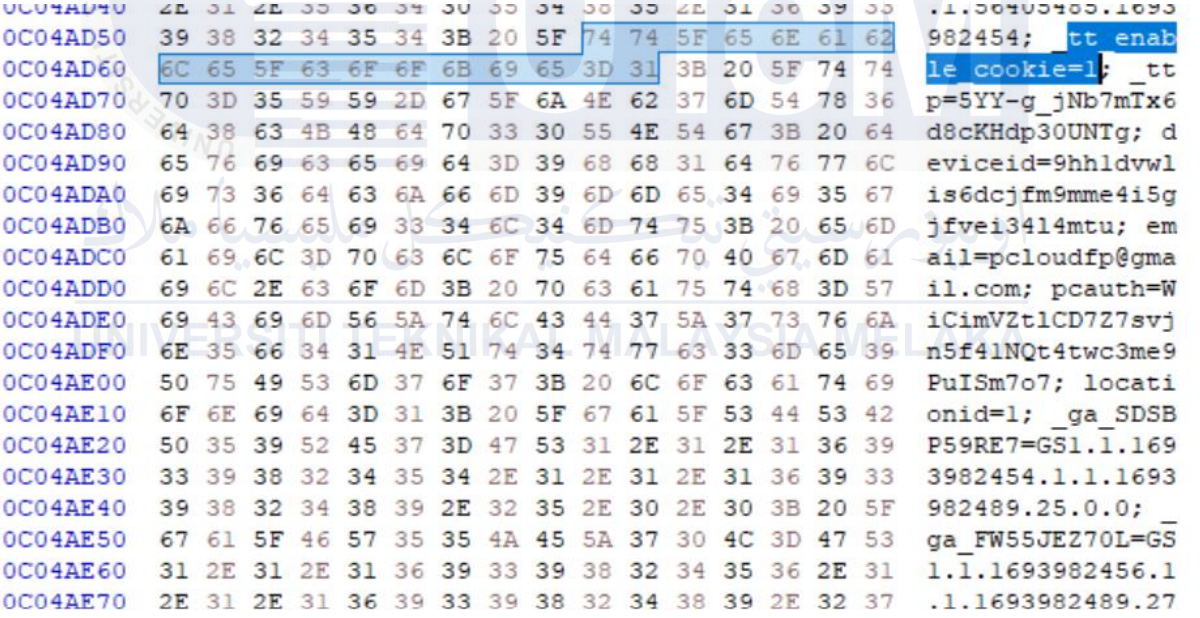


Figure 5.1.1 (4): cookie found in memory.

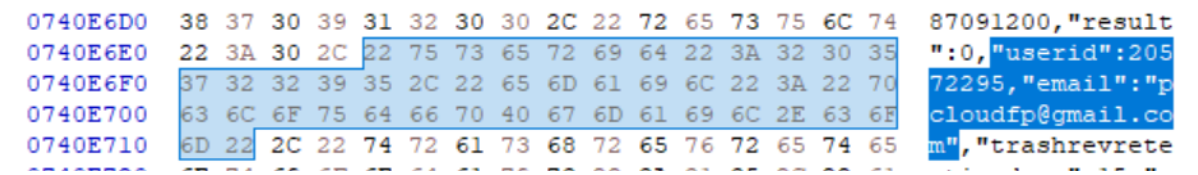


Figure 5.1.1 (5): user id and email found in memory.

Table 5.1.1: Recovered of artifacts in Login process for Web Browser-Based Experiments

Location	**Recovered artifacts**
Cache chrome	email=pcloudfp%40gmail.com
URL	https://eapi.pcloud.com/user/preparelogin?email=pcloudfp%40gmail.com&language=en&os=4
Memory	“email”:pcloudfp@gmail.com
	“userid”:20572295
	Pcloud_test0908 [email password]
	tt_enable_cookie=1; _ttp=5YY-g_jNb7mTx6d8cKHdp30UNTg; deviceid=9hh1dvwlis6dcjfm9mme4i5gjfvei34l4mtu; email=pcloudfp@gmail.com; pcauth=WiCimVZtlCD7Z7svjn5f41NQt4twc3me9PuISm7o7; locationid=1; _ga_SDSBP59RE7=GS1.1.1693982454.1.1.1693982489.25.0.0; _ga_6F200QN94G=GS1.1.1693982456.1.1.1693982489.27.0.0; _ga_FW55JEZ70L=GS1.1.1693982456.1.1.1693982496.20.0.0wc3me9PuISm7o7; locationid=1

5.1.2 Upload

Chromecacheview, folder id and name of of the folder uploaded in pCloud storage was exposed and cached in chrome browser via URL (https://api.pcloud.com/createfolderifnotexists?folderid=18725653427&name=test&auth=pPt2bXZtlCD7ZeSturpNzdkBBc6RH4EvpbYbuwWh7). These remnants can be used to analyse furthermore information related to the folder id and the folder name.

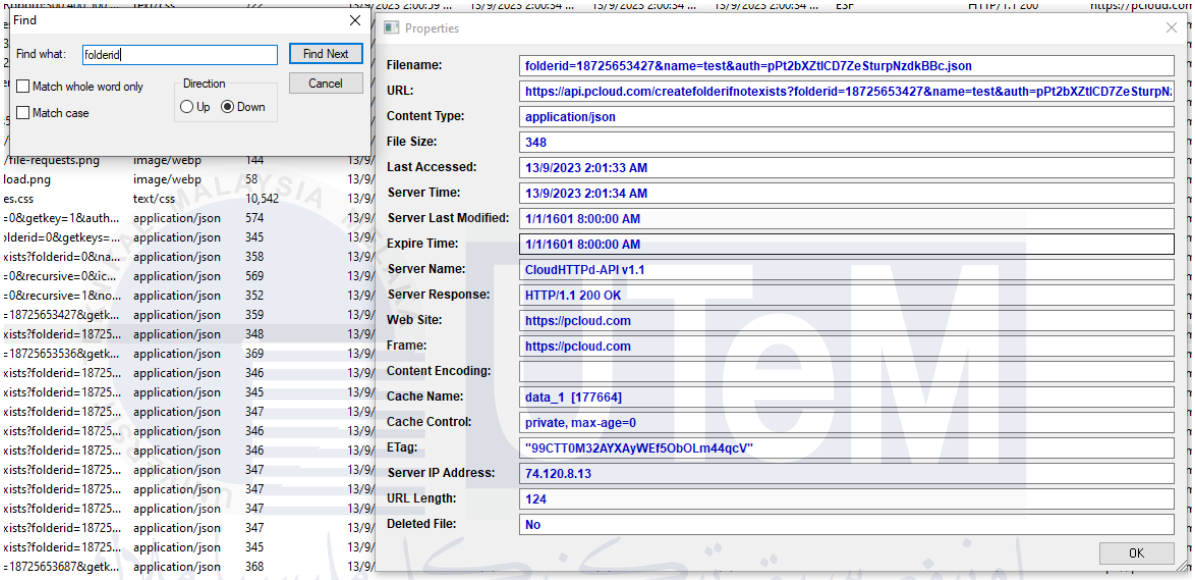


Figure 5.1.2 (1): upload folder is cache in chrome.

Livememory, in the upload process, the dataset folder named “test” was uploaded to the pCloud. In the process of uploading, each file in the folder is uploaded individually. In the analysis, artifacts that are discovered are the name of folder created, name of current files upload, http request of the files, and the leak of file content. However, by using process dump file the leak content cannot be discovered.

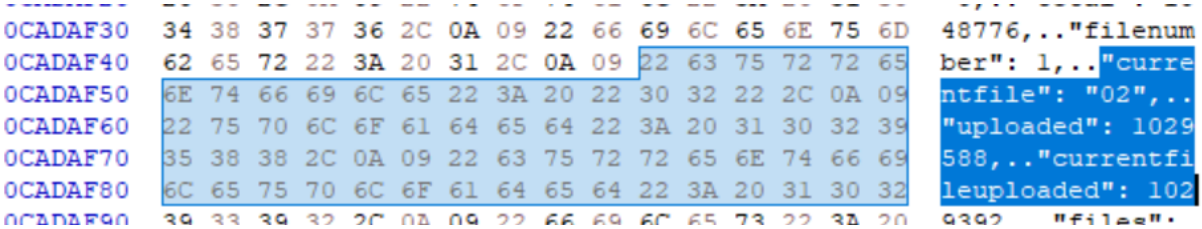
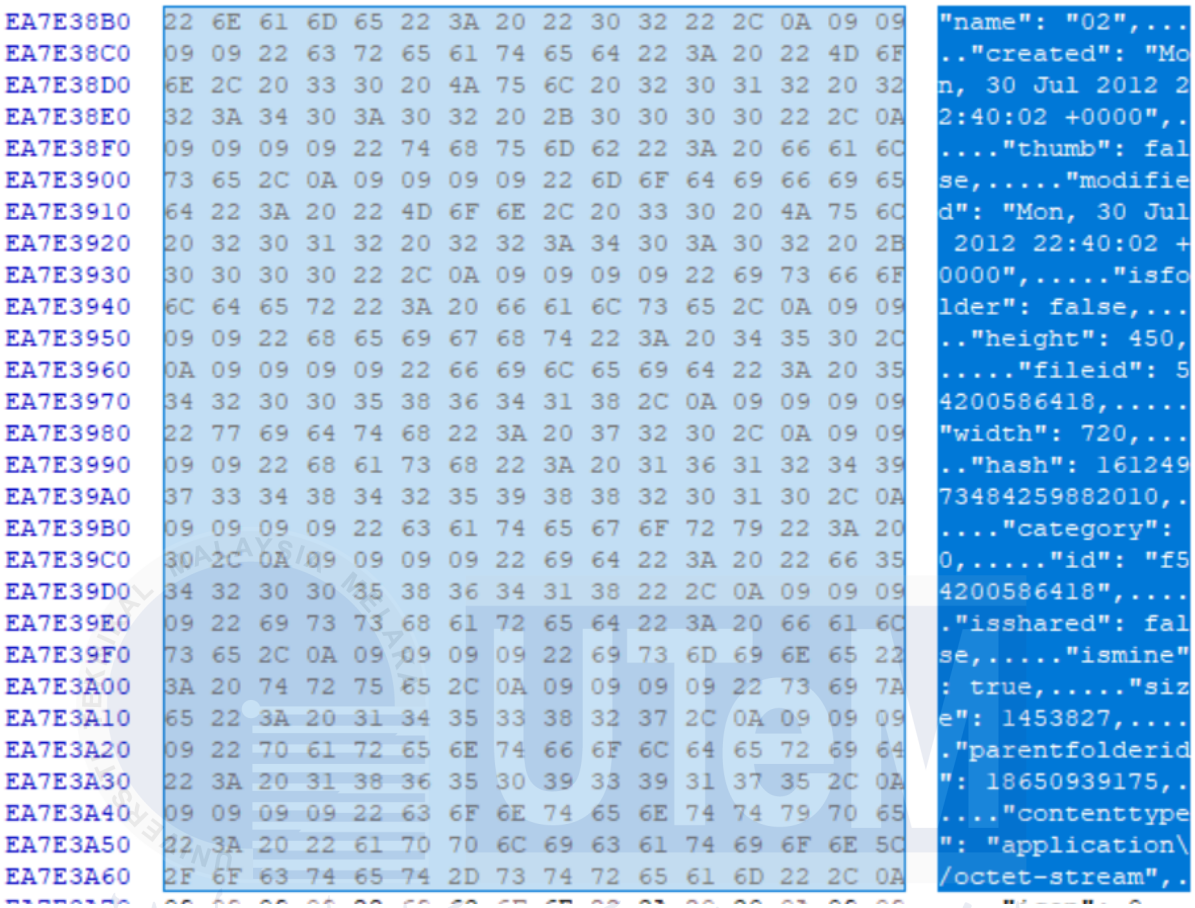
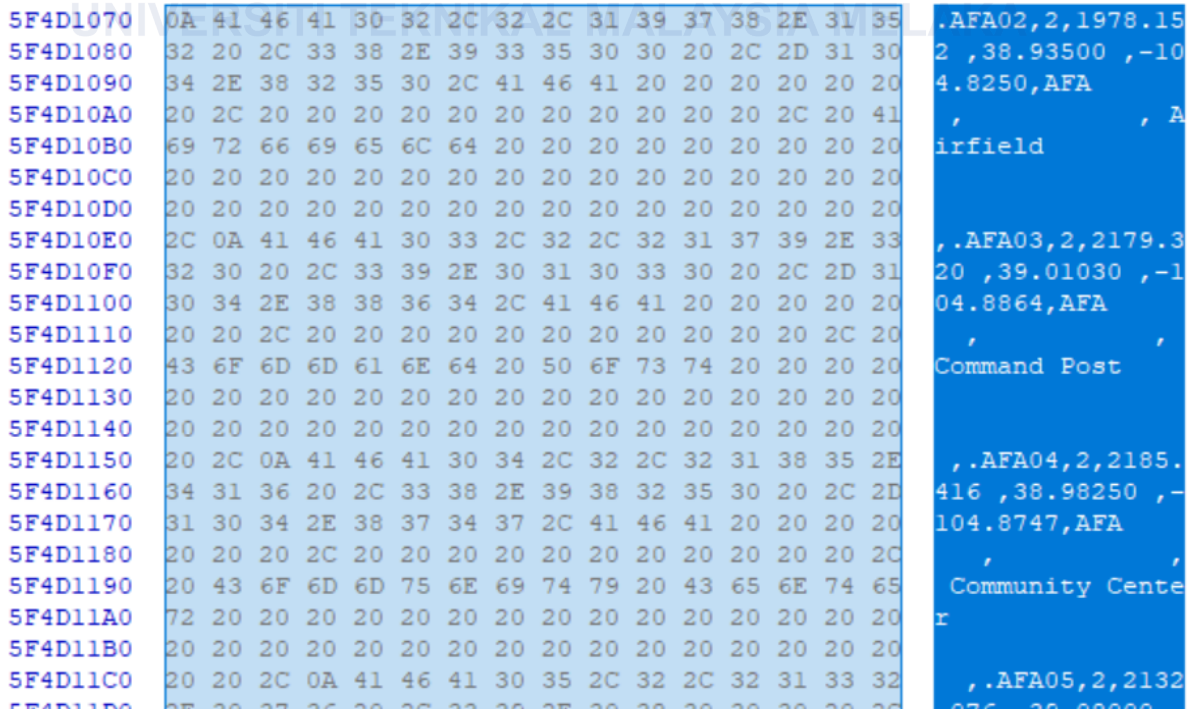


Figure 5.1.2 (2): Name of current file upload



```
EA7E38B0  22 6E 61 6D 65 22 3A 20 22 30 32 22 2C 0A 09 09  "name": "02",...
EA7E38C0  09 09 22 63 72 65 61 74 65 64 22 3A 20 22 4D 6F  ..."created": "Mo
EA7E38D0  6E 2C 20 33 30 20 4A 75 6C 20 32 30 31 32 20 32  n, 30 Jul 2012 2
EA7E38E0  32 3A 34 30 3A 30 32 20 2B 30 30 30 30 22 2C 0A  2:40:02 +0000",.
EA7E38F0  09 09 09 09 22 74 68 75 6D 62 22 3A 20 66 61 6C  ...."thumb": fal
EA7E3900  73 65 2C 0A 09 09 09 09 22 6D 6F 64 69 66 69 65  se,....."modifie
EA7E3910  64 22 3A 20 22 4D 6F 6E 2C 20 33 30 20 4A 75 6C  d": "Mon, 30 Jul
EA7E3920  20 32 30 31 32 20 32 32 3A 34 30 3A 30 32 20 2B   2012 22:40:02 +
EA7E3930  30 30 30 30 22 2C 0A 09 09 09 09 22 69 73 66 6F  0000",....."isfo
EA7E3940  6C 64 65 72 22 3A 20 66 61 6C 73 65 2C 0A 09 09  lder": false,...
EA7E3950  09 09 22 68 65 69 67 68 74 22 3A 20 34 35 30 2C  ..."height": 450,
EA7E3960  0A 09 09 09 09 22 66 69 6C 65 69 64 22 3A 20 35  ....."fileid": 5
EA7E3970  34 32 30 30 35 38 36 34 31 38 2C 0A 09 09 09 09  4200586418,.....
EA7E3980  22 77 69 64 74 68 22 3A 20 37 32 30 2C 0A 09 09  "width": 720,...
EA7E3990  09 09 22 68 61 73 68 22 3A 20 31 36 31 32 34 39  ..."hash": 161249
EA7E39A0  37 33 34 38 34 32 35 39 38 38 32 30 31 30 2C 0A  73484259882010,.
EA7E39B0  09 09 09 09 22 63 61 74 65 67 6F 72 79 22 3A 20  ...."category":
EA7E39C0  30 2C 0A 09 09 09 09 22 69 64 22 3A 20 22 66 35  0,....."id": "f5
EA7E39D0  34 32 30 30 35 38 36 34 31 38 22 2C 0A 09 09 09  4200586418",....
EA7E39E0  09 22 69 73 73 68 61 72 65 64 22 3A 20 66 61 6C  ."isshared": fal
EA7E39F0  73 65 2C 0A 09 09 09 09 22 69 73 6D 69 6E 65 22  se,....."ismine"
EA7E3A00  3A 20 74 72 75 65 2C 0A 09 09 09 09 22 73 69 7A  : true,....."siz
EA7E3A10  65 22 3A 20 31 34 35 33 38 32 37 2C 0A 09 09 09  e": 1453827,....
EA7E3A20  09 22 70 61 72 65 6E 74 66 6F 6C 64 65 72 69 64  ."parentfolderid
EA7E3A30  22 3A 20 31 38 36 35 30 39 33 39 31 37 35 2C 0A  ": 18650939175,.
EA7E3A40  09 09 09 09 22 63 6F 6E 74 65 6E 74 74 79 70 65  ...."contenttype
EA7E3A50  22 3A 20 22 61 70 70 6C 69 63 61 74 69 6F 6E 5C  ": "application\
EA7E3A60  2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 22 2C 0A  /octet-stream",.
```

Figure 5.1.2 (3): Metadata of file upload



```
5F4D1070  0A 41 46 41 30 32 2C 32 2C 31 39 37 38 2E 31 35  .AFA02,2,1978.15
5F4D1080  32 20 2C 33 38 2E 39 33 35 30 30 20 2C 2D 31 30  2 ,38.93500 ,-10
5F4D1090  34 2E 38 32 35 30 2C 41 46 41 20 20 20 20 20 20  4.8250,AFA
5F4D10A0  20 2C 20 20 20 20 20 20 20 20 20 20 20 20 2C 20 41  ,            , A
5F4D10B0  69 72 66 69 65 6C 64 20 20 20 20 20 20 20 20 20  irfield
5F4D10C0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
5F4D10D0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
5F4D10E0  2C 0A 41 46 41 30 33 2C 32 2C 32 31 37 39 2E 33  ,.AFA03,2,2179.3
5F4D10F0  32 30 20 2C 33 39 2E 30 31 30 33 30 20 2C 2D 31  20 ,39.01030 ,-1
5F4D1100  30 34 2E 38 38 36 34 2C 41 46 41 20 20 20 20 20  04.8864,AFA
5F4D1110  20 20 2C 20 20 20 20 20 20 20 20 20 20 20 20 2C 20  ,            ,
5F4D1120  43 6F 6D 6D 61 6E 64 20 50 6F 73 74 20 20 20 20  Command Post
5F4D1130  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
5F4D1140  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
5F4D1150  20 2C 0A 41 46 41 30 34 2C 32 2C 32 31 38 35 2E  ,.AFA04,2,2185.
5F4D1160  34 31 36 20 2C 33 38 2E 39 38 32 35 30 20 2C 2D  416 ,38.98250 ,-
5F4D1170  31 30 34 2E 38 37 34 37 2C 41 46 41 20 20 20 20  104.8747,AFA
5F4D1180  20 20 20 2C 20 20 20 20 20 20 20 20 20 20 20 2C  ,            ,
5F4D1190  20 43 6F 6D 6D 75 6E 69 74 79 20 43 65 6E 74 65  Community Cente
5F4D11A0  72 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  r
5F4D11B0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
5F4D11C0  20 20 2C 0A 41 46 41 30 35 2C 32 2C 32 31 33 32  ,.AFA05,2,2132
```

Figure 5.1.2 (4): Leak file content when uploading.

Table 5.1.2: Recovered of artifacts in Upload process for Web Browser-Based Experiments

Location	Recovered artifacts
Chrome cache	folderid=18725653427
	name=test
URL	https://api.pcloud.com/createfolderifnotexists?folderid=18725653427&name=test&auth=pPt2bXZtlCD7ZeSturpNzdkBBc6RH4EvpbYbuwWh7
Memory	"currentfile": "02"
	"name": "02"
	"created": "Mon, 30 Jul 2012 22:40:02 +0000"
	"fileid": 54200586418
	"hash": 16124973484259882010

5.1.3 Download and Open

In this analysis the download process is using the new uploaded file “fig-03.gif”, the file chosen is from the dataset with the change of file name to make sure the process can be seen clearly.

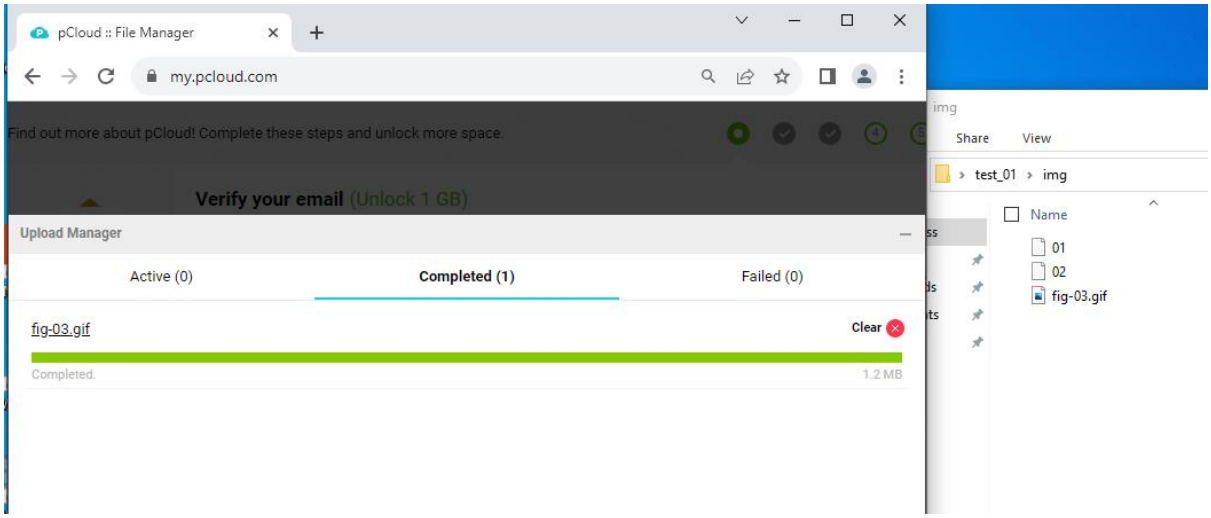


Figure 5.1.3 (1): New file uploaded in pCloud for download process.

Hashcalc, in this phase shows that the file that is uploaded to pCloud does not undergo any changes of its content and metadata. The hash value of both files before it was uploaded to pCloud and after it was downloaded are the same. By using exiftool, it reveals the metadata of the file are the same for both files before it was uploaded to pCloud and after it was downloaded.

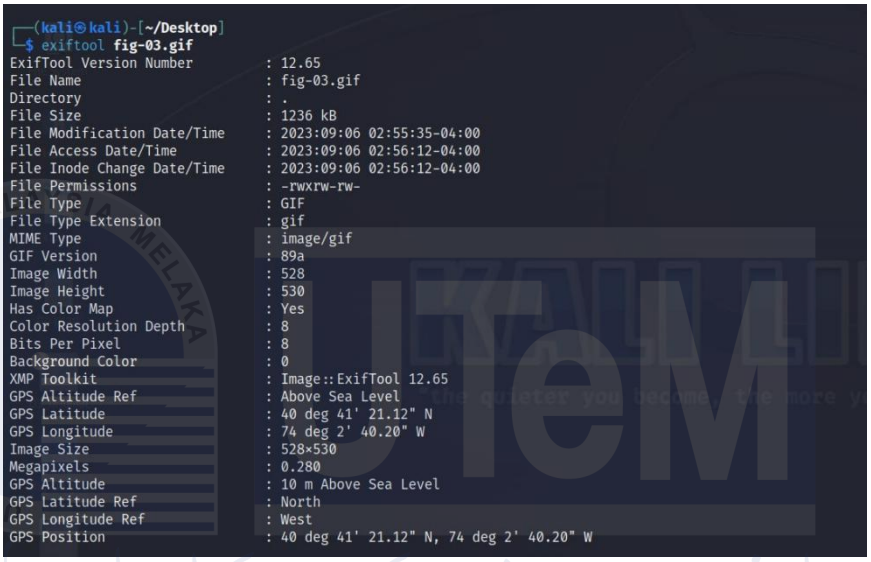


Figure 5.1.3 (2): metadata of file before upload

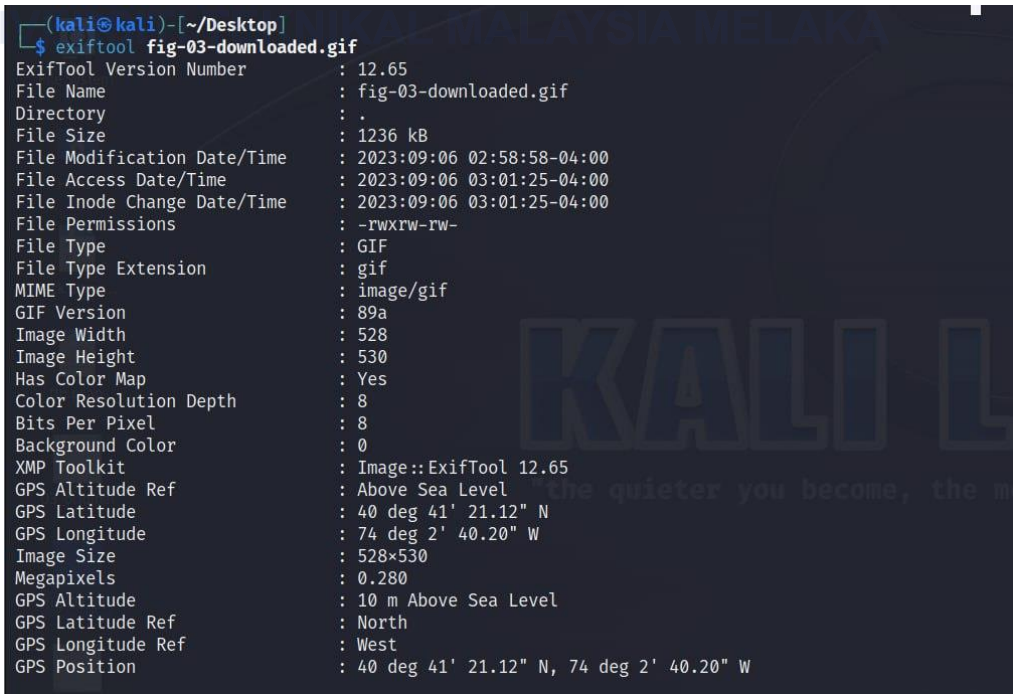


Figure 5.1.3 (3): Metadata of the file after upload

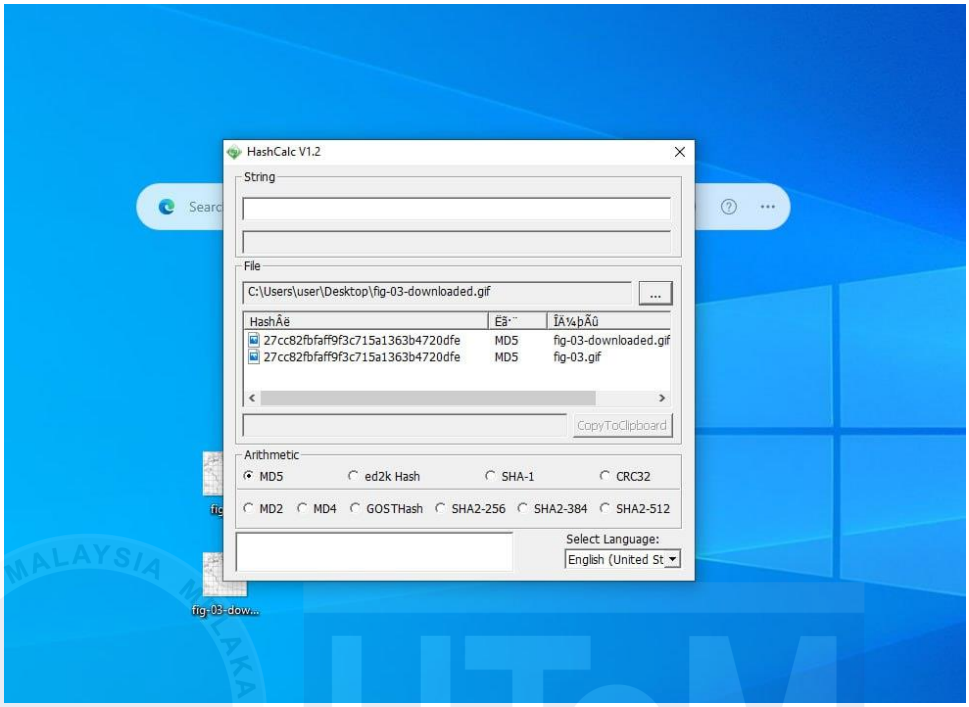


Figure 5.1.3 (4): Hash value of both files before and after downloaded.

Livememory, in download case, both virtual memory and process dump files found the same artifacts; name of the file downloaded with the metadata, path of the file download, and leak content of files by using hex values. In this case, the file downloaded is .gif, to find the content of the file, keywords for the file signature are used.


```
798ADB00  02 00 00 00 2E 01 00 00 01 EA C4 54 7B 0A 09 22  ........eÄT{..."
798ADB10  72 65 73 75 6C 74 22 3A 20 30 2C 0A 09 22 64 77  result": 0,.."dw
798ADB20  6C 74 61 67 22 3A 20 22 31 38 79 70 42 72 78 58  ltag": "18ypBrxX
798ADB30  67 43 7A 36 33 47 69 46 76 53 50 37 7A 6A 22 2C  gCz63GiFvSP7zj",
798ADB40  0A 09 22 68 61 73 68 22 3A 20 34 34 38 37 37 34  .."hash": 448774
798ADB50  35 31 36 34 36 31 35 30 34 37 36 30 32 2C 0A 09  5164615047602,..
798ADB60  22 73 69 7A 65 22 3A 20 31 32 33 33 30 31 32 2C  "size": 1233012,
798ADB70  0A 09 22 65 78 70 69 72 65 73 22 3A 20 22 57 65  .."expires": "We
798ADB80  64 2C 20 30 36 20 53 65 70 20 32 30 32 33 20 32  d, 06 Sep 2023 2
798ADB90  32 3A 32 36 3A 30 30 20 2B 30 30 30 30 22 2C 0A  2:26:00 +0000",.
798ADBA0  09 22 70 61 74 68 22 3A 20 22 5C 2F 64 70 5A 49  ."path": "\/dpZI
798ADBB0  6A 32 79 45 74 5A 4E 56 4B 6E 7A 58 37 5A 74 6C  j2yEtZNVKnzX7Ztl
798ADBC0  43 44 37 5A 5A 45 44 53 53 79 6B 5A 32 5A 5A 6A  CD7ZZEDSSykZ2ZZj
798ADBD0  33 37 5A 5A 4D 6E 39 61 44 50 73 43 36 47 75 35  37ZZMn9aDPsC6Gu5
798ADBE0  61 7A 57 7A 56 50 58 39 4F 34 32 44 53 7A 6D 37  azWzVPX9O42DSzm7
798ADBF0  5C 2F 66 69 67 2D 30 33 2E 67 69 66 22 2C 0A 09  \/fig-03.gif",..
798ADC00  22 68 6F 73 74 73 22 3A 20 5B 0A 09 09 22 76 63  "hosts": [..."vc
798ADC10  38 34 31 2E 70 63 6C 6F 75 64 2E 63 6F 6D 22 2C  841.pcloud.com",
798ADC20  0A 09 09 22 76 63 38 30 32 2E 70 63 6C 6F 75 64  ..."vc802.pcloud
798ADC30  2E 63 6F 6D 22 0A 09 5D 0A 7D 00 00 00 00 00 00  .com"..].}.....
```

Figure 5.1.3 (5): Name of download file with metadata

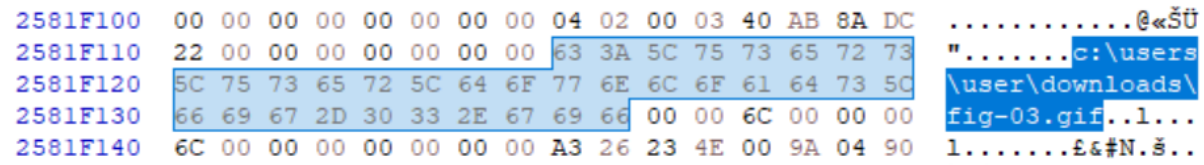


Figure 5.1.3 (6): Path of the download file.

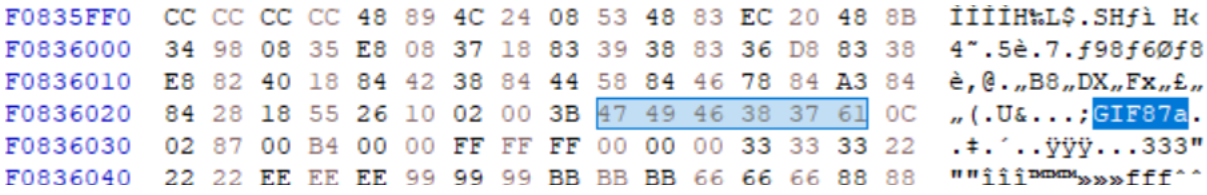


Figure 5.1.3 (7): Leak file content by using hex values.

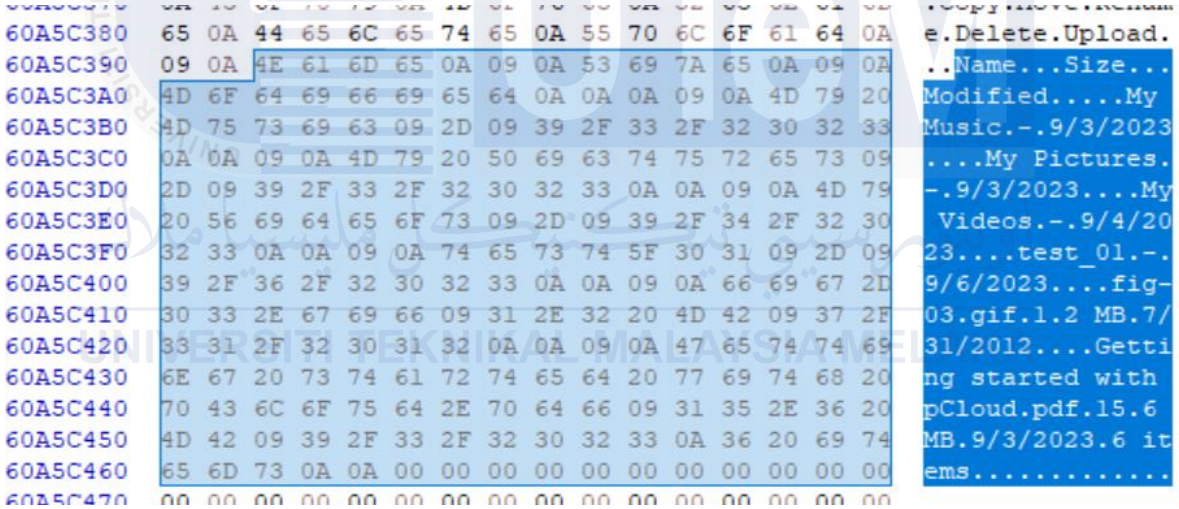


Figure 5.1.3 (8): List of files and folders in the pCloud storage.

Table 5.1.3: Recovered of artifacts in Download and Open process for Web Browser-Based Experiments

Location	Recovered artifacts
Memory	"hash": 4487745164615047602
	"size": 1233012
	"expires": "Wed, 06 Sep 2023 22:26:00 +0000"

	"path": "\/dpZIj2yEtZNVKnzX7ZtlCD7ZZEDSSykZ2ZZj37ZZMn9aDPsC6Gu5azWzVPX9O42DSzm7\/fig-03.gif"
	C:\Users\User\Downloads\fig-03.gif
	My Music - 9/3/2023 My Pictures - 9/3/2023 My Videos - 9/4/2023 test_01 - 9/6/2023 fig-03.gif 1.2 MB 7/31/2012 Getting started with pCloud.pdf 15.6 MB 9/3/2023

5.1.4 Delete

In this delete process, analysis is made to search if there is remnants left if any files or folders deleted permanently in the pCloud storage.

Chromecacheview, file id and file name of the deleted file was exposed and cached in chrome browser via URL (https://api.pcloud.com/deletefile?fileid=54396532871&name=pdf-01-512-gt&id=574-0&auth=JGhY6XZtlCD7ZsANGHwGLKeSRbL3TtGIS4ugoR0qV). The remnants gained could be used in further analysis that are tied with the deleted file id and file name.

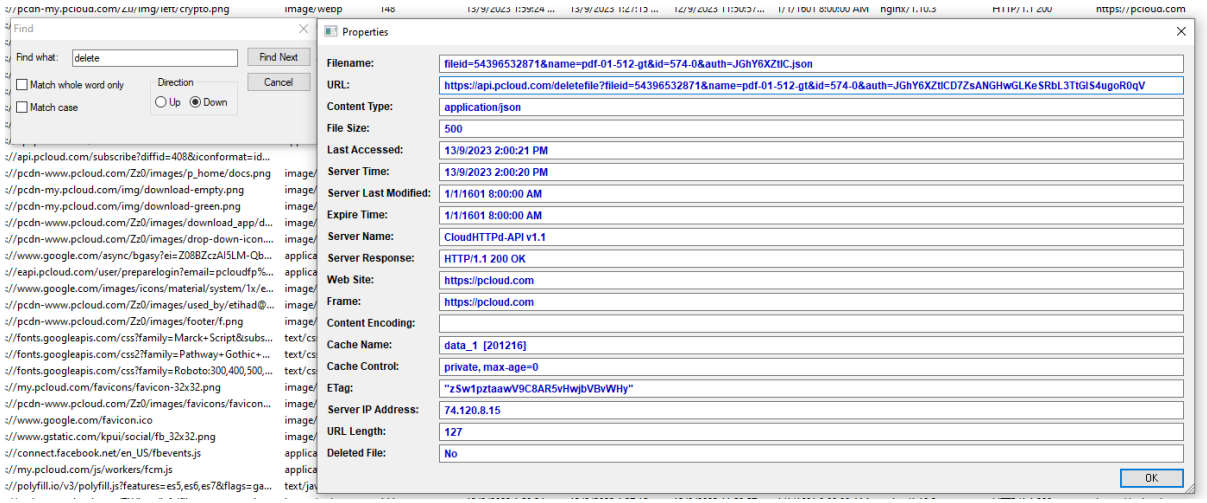


Figure 5.1.4 (1): Chromecacheview

Livememory, in the virual memory and process dump files, the URL of the delete file is found, in the URL another information can be obtained; file id and file name. Another artifact found in the virtual memory file is the event of the deleted file is stated.

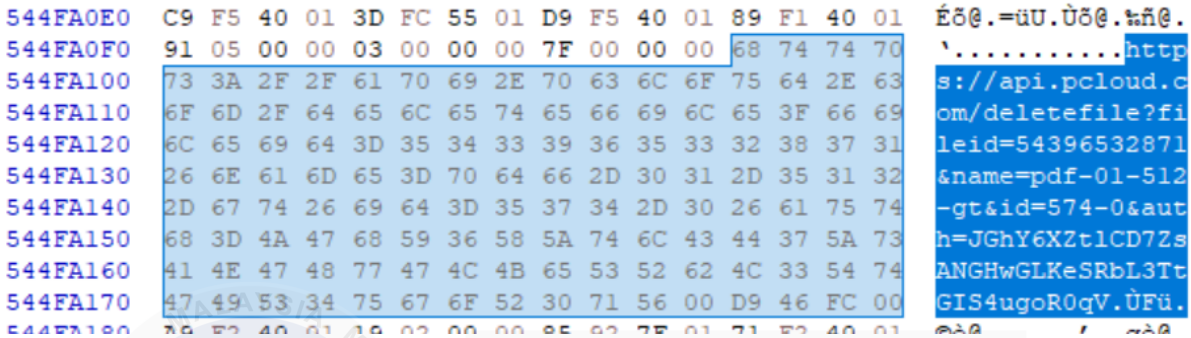


Figure 5.1.4 (2): URL of the deleted file

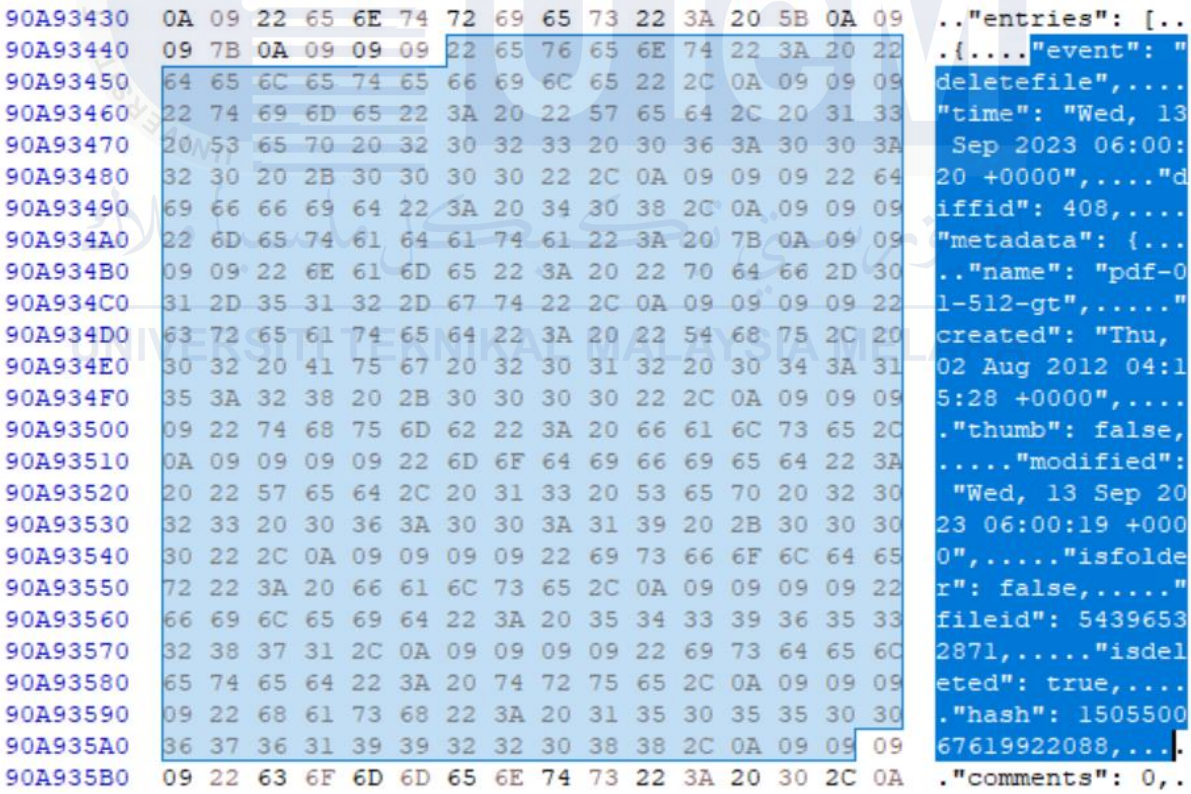


Figure 5.1.4 (3): Information about deleted files.

Table 5.1.4: Recovered of artifacts in Delete process for Web Browser-Based Experiments

Location	**Recovered artifacts**
Chrome cache	fileid=54396532871
	name=pdf-01-512-gt
URL	https://api.pcloud.com/deletefile?fileid=54396532871&name=pdf-01-512-gt&id=574-0&auth=JGhY6XZtlCD7ZsANGHwGLKeSRbL3TtGIS4ugoR0qV
Memory	"event": "deletefile"
	"time": "Wed, 13 Sep 2023 06:00:20 +0000"
	"name": "pdf-01-512-gt"
	"created": "Thu, 02 Aug 2012 04:15:28 +0000",

5.2 Windows App-Based Experiments

In this section, the evidential data obtained from the analysis of the pCloud application installed on a Windows OS is discussed. Three specific tasks are explained: installation and login, upload, download, delete, and uninstallation.

5.2.1 Installation and Login

Upon the first installation of the pCloud on Windows, we have traced down the changes that the app made on both file system and the registry of the computer. The pCloud client created and modified the following address on the disk drive: C:\Program Files\pCloud Drive\. This address is used to store the pCloud client files, the configuration, and some other necessary files. Other than the system's disk drive, pCloud has created entries in the registry of the Windows. The Registry entries can be found in the following locations:

Table 5.2.1 (1): Registry key added for installation.

Registry key added
• HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CurVer • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1 • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CurVer • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1 • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\CLSID • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINPROGRESS • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINSYNC • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudNOSYNC • HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud • HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\pCloud Drive

Table 5.2.1 (2): Registry values added.

Values added
• HKLM\SOFTWARE\Classes\CLSID\{063B8D8A-E610-3800-92BF-D2AF9DCDAB85}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{063B8D8A-E610-3800-92BF-D2AF9DCDAB85}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{3103A792-C2D9-3C57-98DD-30071B26C05F}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{3103A792-C2D9-3C57-98DD-30071B26C05F}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\: "pCloudNOSYNC Class" • HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll" • HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\ProgID\: "OverlayIcon.pCloudNoSync.1" • HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\VersionIndependentProgID\: "OverlayIcon.pCloudNOSYNC" • HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\: "pCloudINSYNC Class" • HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll" • HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\ProgID\: "OverlayIcon.pCloudINSYNC.1" • HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\VersionIndependentProgID\: "OverlayIcon.pCloudINSYNC" • HKLM\SOFTWARE\Classes\CLSID\{A2D0C838-9DD7-35F6-A64B-0828607D8422}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{A2D0C838-9DD7-35F6-A64B-0828607D8422}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\: "pCloud_INPROGRESS Class" • HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll" • HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\ProgID\: "OverlayIcon.pCloudInProgress.1"

- HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\VersionIndependentProgID\: "OverlayIcon.pCloud_INPROGRESS"
- HKLM\SOFTWARE\Classes\Installer\Dependencies\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Dependencies\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Products\8A51FA49EEEB89D43B0DD7C705825BA3\ProductName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Products\8A51FA49EEEB89D43B0DD7C705825BA3\SourceList\PackageName: "pCloud Drive.msi"
- HKLM\SOFTWARE\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SOFTWARE\Classes\WOW6432Node\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\WOW6432Node\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon\: "pCloudINSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon\CurVer\: "OverlayIcon.pCloudINSYNC.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon.1\: "pCloudINSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\: "pCloud_INPROGRESS Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CLSID\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CurVer\: "OverlayIcon.pCloudInProgress.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\: "pCloud_INPROGRESS Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\CLSID\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\: "pCloudNOSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CLSID\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CurVer\: "OverlayIcon.pCloudNoSync.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\: "pCloudNOSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\CLSID\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINPROGRESS\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINSYNC\: "{8D0C0582-552A-4A6B-9455-DA63E1F329C0}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudNOSYNC\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\: "1"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\de\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\es\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\fr\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\ja\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\nl\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\dbg\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\rls\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\zh\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\17BCFBB5AC9A9BB4DA3F4B9C7E9331D8\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\ja\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\225192B6419CBBC4CAA1240908BE7170\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\pthreadVC2.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\410ECE1A32F741440B444504863D4ADD\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\pCloud.exe"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\584D9B900B1D5FB4B99BBE67C7738FDD\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\nl\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\83654B787874C4244B5733C954CE04EF\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\Microsoft\Windows\CurrentVersion\Run\pCloud"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\83654B787874C4244B5733C954CE04EF\00000000000000000000000000000000: "21:\Software\Microsoft\Windows\CurrentVersion\Run\pCloud"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8AA2B6BC4C59484558BCB8B828C5B0D8\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\pCloud\pCloud Drive\installed"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\9818DD341F2E62A4B9B65E9B1CA4496D\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\fr\ContextMenuHandler.resources.dll"

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B8991F4234EFEBC4F8A2180B2B003A2C\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\pCloud\AppPath"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B8991F4234EFEBC4F8A2180B2B003A2C\00000000000000000000000000000000: "21:\Software\pCloud\AppPath"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C007ED4F4337DDD47A7E6E2E0E4846BE\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\dbg\pSyncLib.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\DD1F3D05E323BE846819EE4D74518C8C\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\es\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\DE320DED86BA4A540901A6DBCE880357\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\E3444181A32776E4EB5F57153E4787A5\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\de\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\EC22AAA47CDD9B546A11C98BF67313CB\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\zh\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F1439F25836095E469596EF5C547CAD5\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\ContextMenuHandler.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FDA3EC1B3490B5B409727AFB119AA409\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\rls\pSyncLib.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8A51FA49EEEB89D43B0DD7C705825BA3\InstallProperties\Publisher: "pCloud AG"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8A51FA49EEEB89D43B0DD7C705825BA3\InstallProperties\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\Publisher: "pCloud AG"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\BundleCachePath: "C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe"

- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayIcon: "C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe,0"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\Publisher: "pCloud AG"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\ModifyPath: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /modify"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\QuietUninstallString: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /uninstall /quiet"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\UninstallString: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /uninstall"
- HKLM\SOFTWARE\WOW6432Node\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\WOW6432Node\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Users\user\AppData\Local\Temp\{19A519A9-B4BB-46EB-90CD-D12B4E1B41B4}\.cr\pCloud_Windows_4.1.3_x64.exe: F8 62 8C 47 79 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Users\user\AppData\Local\Temp\{0009AE83-551D-4319-B6A8-27E8474BDE82}\.be\pCloud Drive.exe: 4C 63 6D 47 79 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program Files\pCloud Drive\pCloud.exe: B2 DD 52 C3 7A DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\ControlSet001\Services\cbfs20\Guid-cbfs20-pCloud Drive: 0x00000001
- HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{099B27BE-90F5-4CBC-84FC-362B97DA3635}: "v2.30|Action=Allow|Active=TRUE|Dir=In|RA4=LocalSubnet|RA6=LocalSubnet|App=C:\Program Files\pCloud Drive\pCloud.exe|Name=PCloud AG|Edge=TRUE|"
- HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Users\user\AppData\Local\Temp\{19A519A9-

B4BB-46EB-90CD-D12B4E1B41B4}\.cr\pCloud_Windows_4.1.3_x64.exe: F8 62 8C 47 79 DE 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-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Users\user\AppData\Local\Temp\{0009AE83-551D-4319-B6A8-27E8474BDE82}\.be\pCloud Drive.exe: 4C 63 6D 47 79 DE 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-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program Files\pCloud Drive\pCloud.exe: B2 DD 52 C3 7A DE D9 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\CurrentControlSet\Services\cbfs20\Guid-cbfs20-pCloud Drive: 0x00000001
- HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{099B27BE-90F5-4CBC-84FC-362B97DA3635}: "v2.30|Action=Allow|Active=TRUE|Dir=In|RA4=LocalSubnet|RA6=LocalSubnet|App=C:\Program Files\pCloud Drive\pCloud.exe|Name=PCloud AG|Edge=TRUE|"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppBadgeUpdated\{6D809377-6AF0-444B-8957-A3773F02200E}\pCloud Drive\pCloud.exe: 0x0000000A
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pCloud: "C:\Program Files\pCloud Drive\pCloud.exe"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\user\Downloads\pCloud_Windows_4.1.3_x64.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 48 0C D4 05 63 A9 D4 05 01 00 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 50 BB 64 ED DD AC D5 01 00 00 00 00 00 00 00 00
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\AppPath: "C:\Program Files\pCloud Drive\pCloud.exe"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\ShellExt: "True"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\Logged: "True"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\lang: "en-US"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\SyncDrive: "P:\"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\pCloud Drive\installed: 0x00000001

Database, from registry database file is created, thus from the created file, a lot of information gained from the file such as the information of the account, the metadata of files in cloud storage. The tools use to extract the database file is DB browser for SQLITE

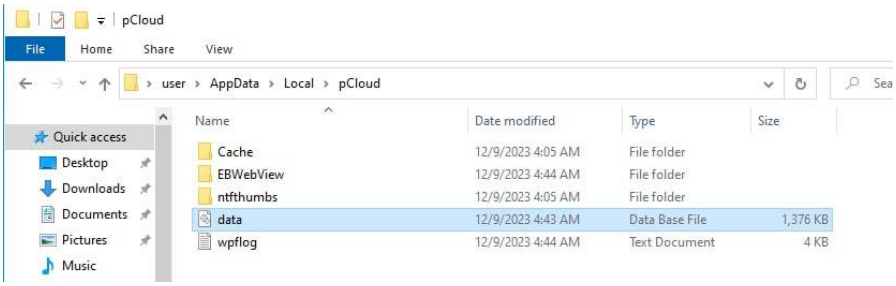


Figure 5.2.1 (1): database file

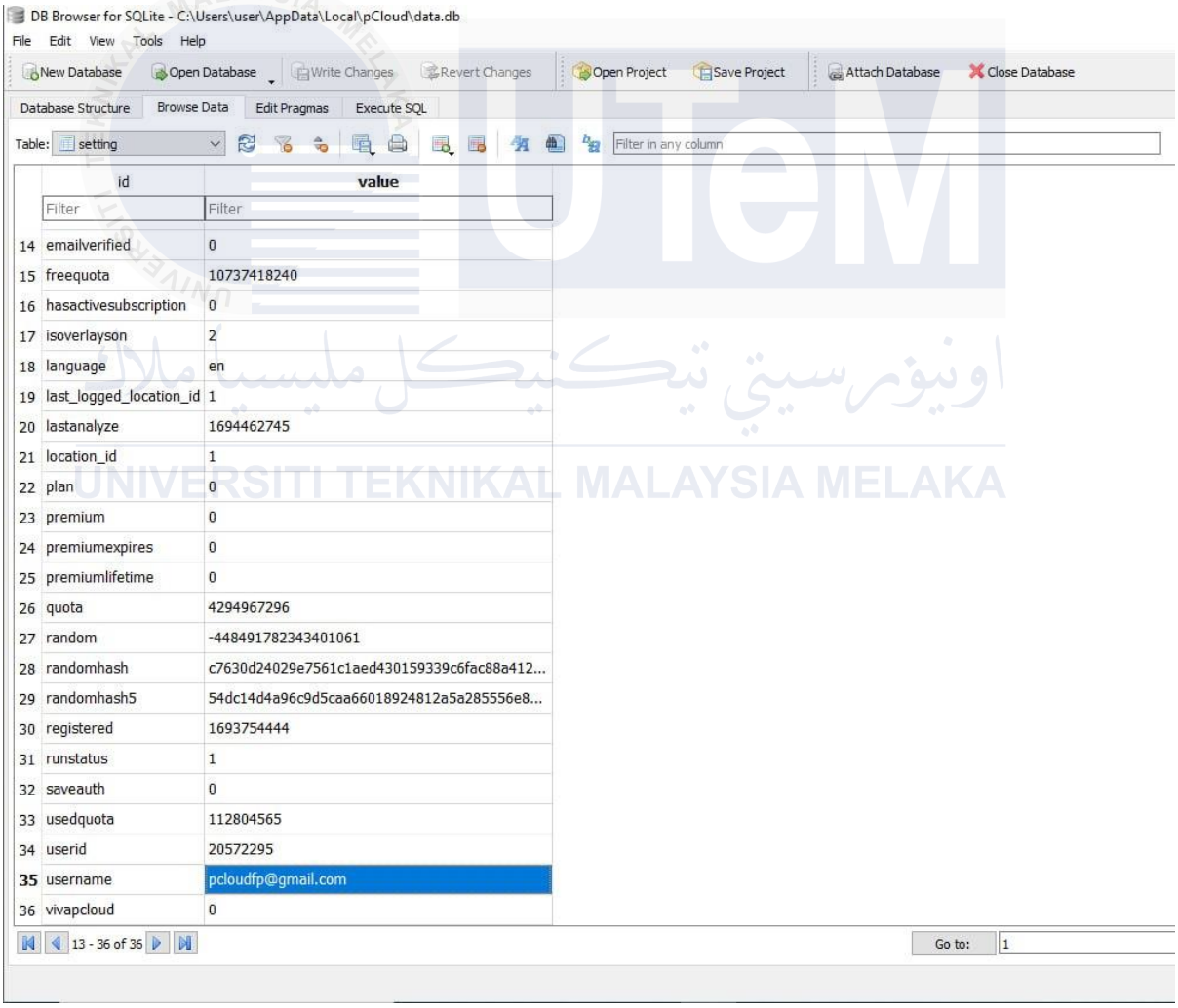


Figure 5.2.1 (2): Setting table.

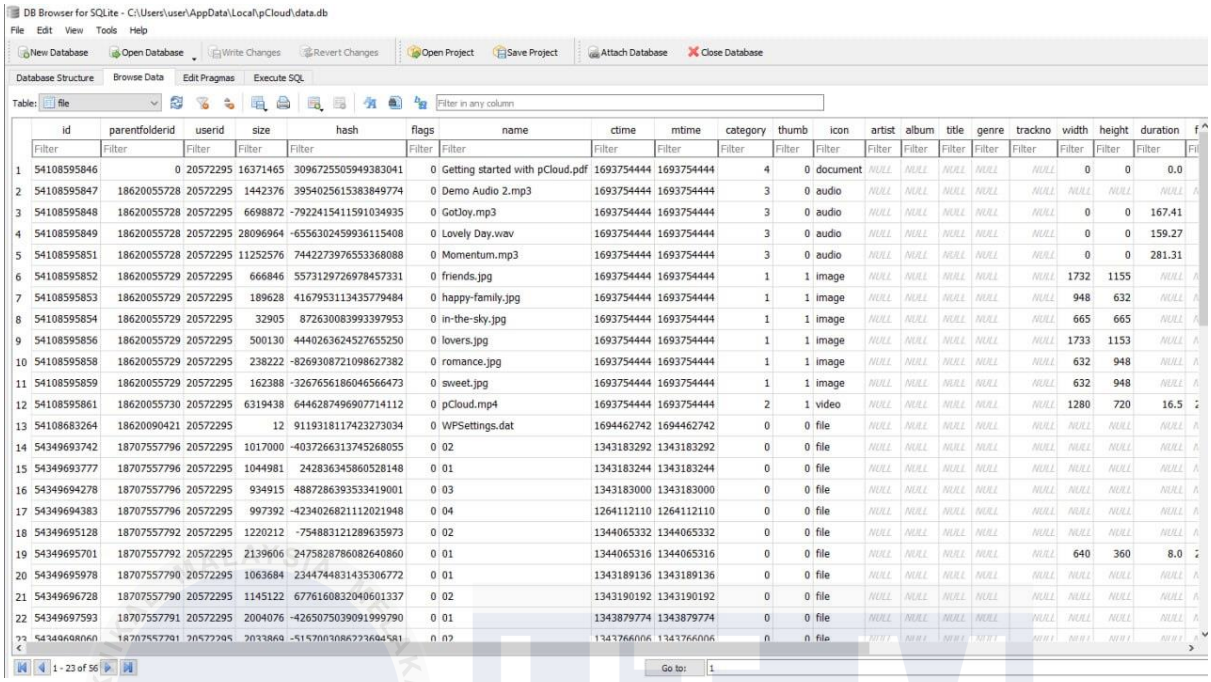


Figure 5.2.1 (3): File table

Livememory, During the login process, identifiable artifacts such as the username, password, and the pCloud directory can serve as substantial evidence of the user's login activity on the device.

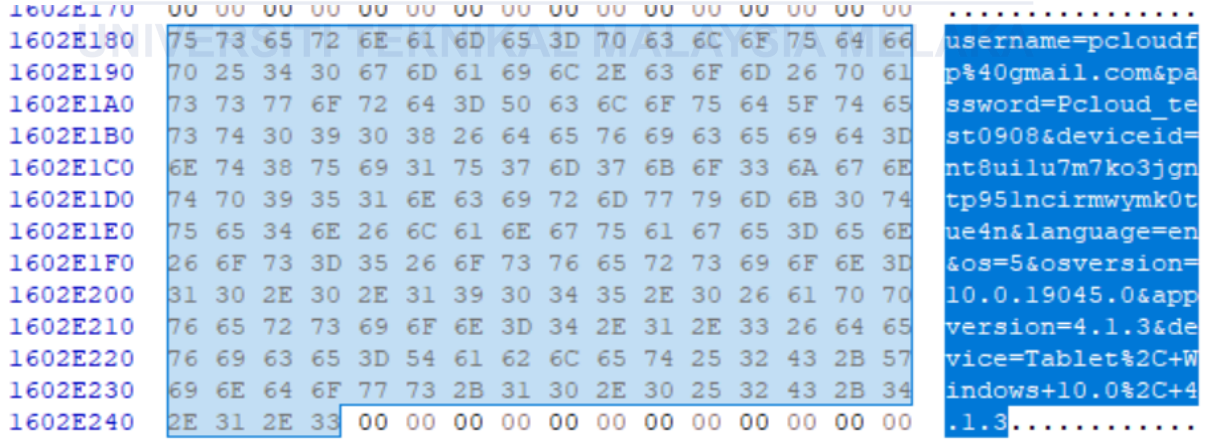


Figure 5.2.1 (4): username and password in virtual memory.

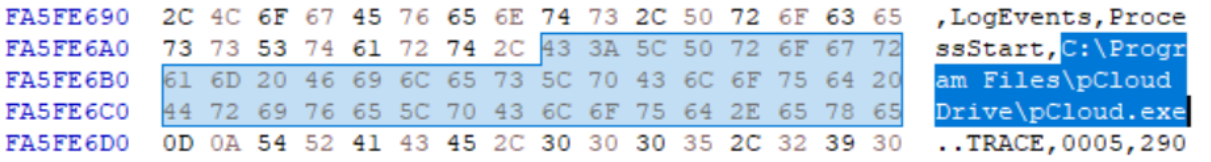


Figure 5.2.1 (5): Directory of pCloud in virtual memory.

Table 5.2.1 (3): Recovered artifacts in Login process for Web Browser-Based Experiments.

Location	**Recovered artifacts**
Registry	Based on **Table 5.2.1 (1)** and **Table 5.2.1 (2)**
Data base file	Setting of the account (**Figure 5.2.1(2)**)
	List of files in pCloud (**Figure 5.2.1(3)**)
Memory	username=pcloudfp%gmail.com
	password=Pcloud_test0908
	deviceid= nt8ui1u7m7ko3jgntp951ncirmwymk0tue4n

5.2.2 Upload

Livememory, the upload process involves the discovery of various artifacts, including the username and password, even in the absence of a login process. Additionally, another artifact identified in the virtual memory is the name of the uploaded file along with its leaked content.

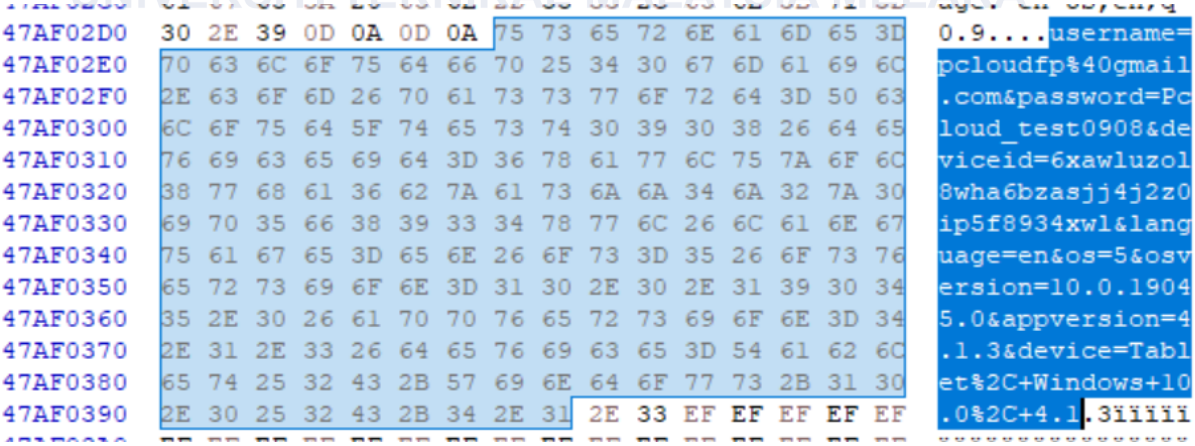


Figure 5.2.2 (1): Username and password in virtual memory.

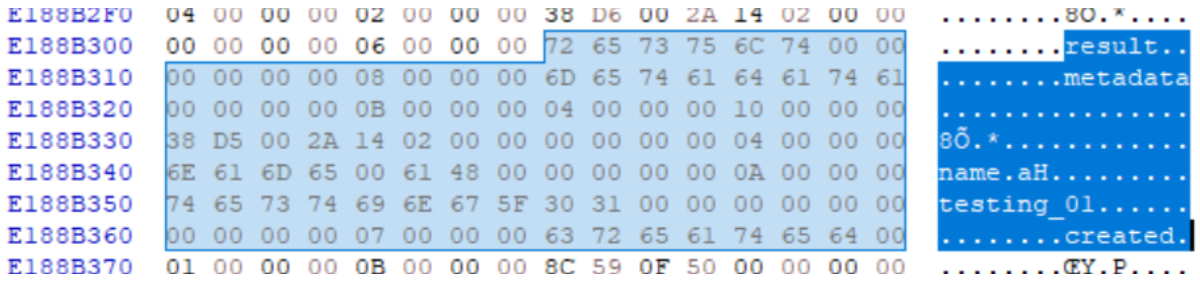


Figure 5.2.2 (2): File name in virtual memory.

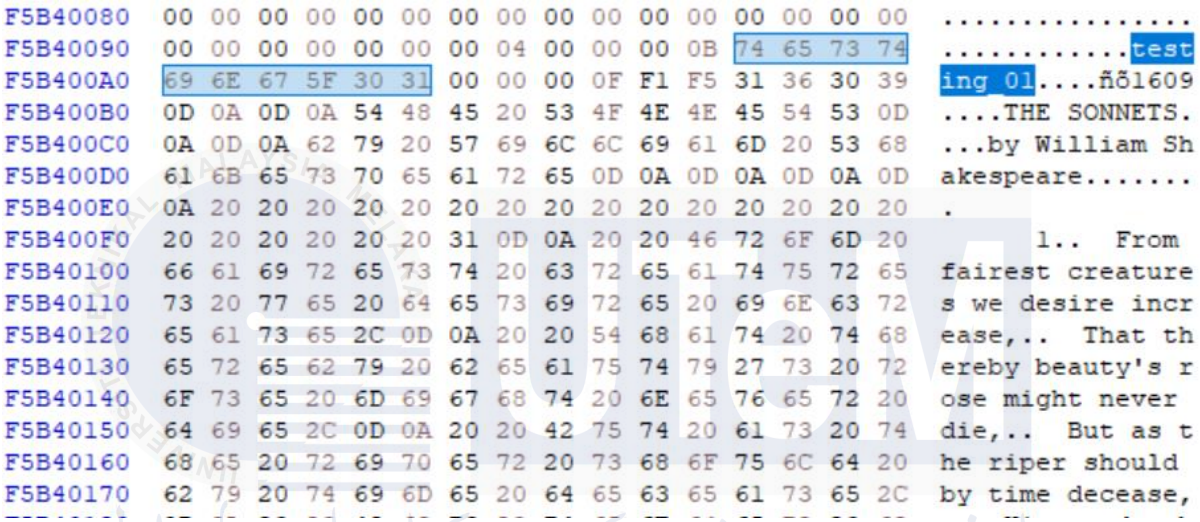


Figure 5.2.2 (3): Upload file content in virtual memory.

Table 5.2.2: Recovered artifacts in Upload process for Web Browser-Based Experiments.

Location	Recovered artifacts
Memory	username=pcloudfp%gmail.com
	password=Pcloud_test0908
	deviceid= 6xawluzol8wha6bzasjj4j2z0ip5f8934xwl
	testing_01 (file name)
	Content file of testing_01

5.2.3 Download and Open

Livememory, numerous artifacts are uncovered during this process, including the username and password, even in the absence of a login procedure. Furthermore, the process reveals details such as the name of the downloaded file and its storage location.

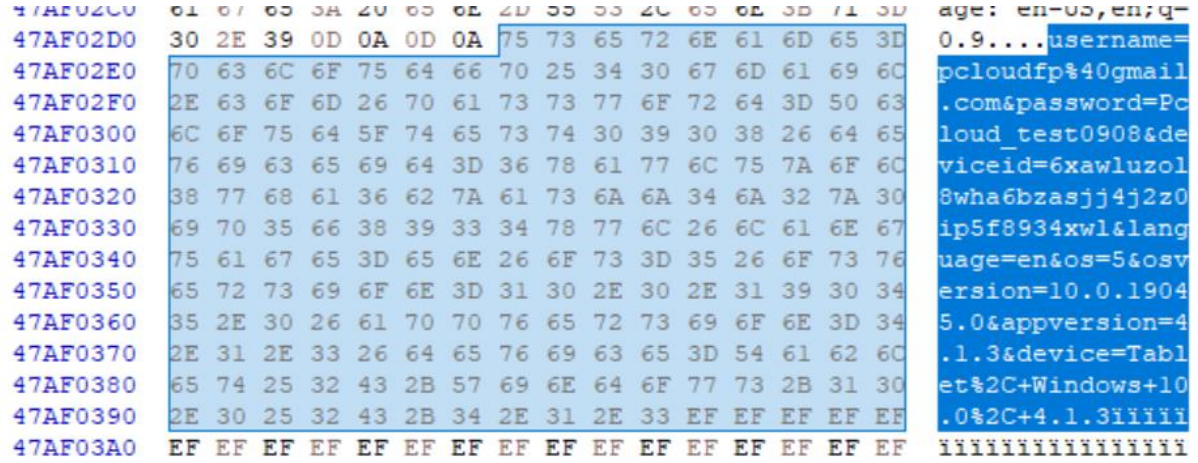


Figure 5.2.3 (1): Username and password in virtual memory.

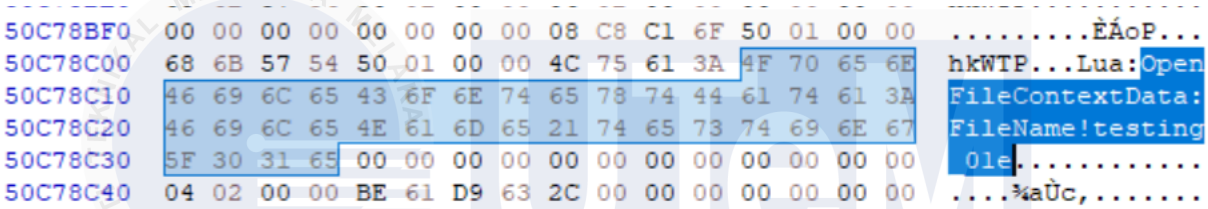


Figure 5.2.3 (2): File name in virtual memory.

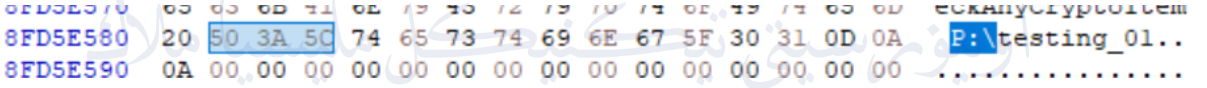


Figure 5.2.3 (3): Location of file in virtual memory.

Table 5.2.3: Recovered artifacts in Download and open process for Web Browser-Based Experiments.

Location	Recovered artifacts
Memory	username=pcloudfp%gmail.com
	password=Pcloud_test0908
	deviceid= 6xawluzol8wha6bzasjj4j2z0ip5f8934xwl
	testing_01 (file name)
	P:\testing_01 (location of file)

5.2.4 Delete

Livememory, artifacts uncovered during this delete process is the location of file and in virtual memory.

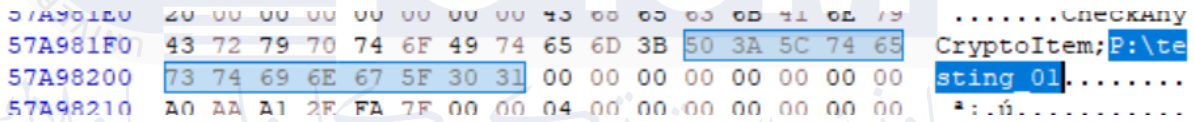


Figure 5.2.4 (1): Location of file in virtual memory.

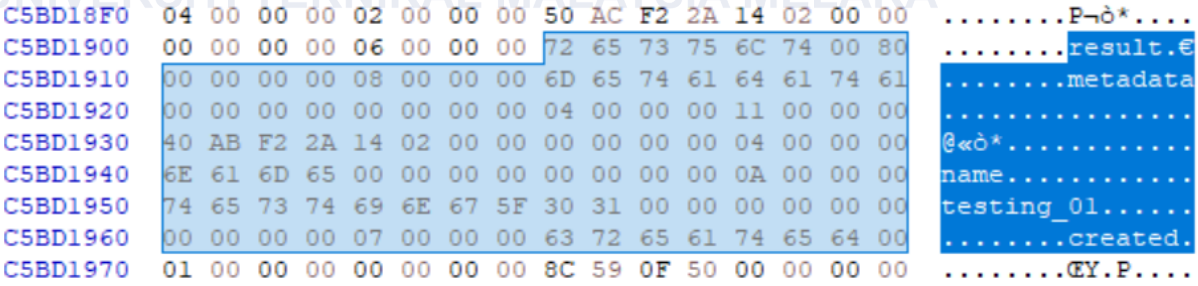


Figure 5.2.4 (2): File in virtual memory.

Table 5.2.4: Recovered of artifacts in Delete process for Web Browser-Based Experiments.

Location	Recovered artifacts
Memory	testing_01 (file name)
	P:\testing_01 (location of file)

5.2.5 Uninstallation

During uninstallation, the registry keys and values are being observed to identify changes. Below are the keys and values that is added and deleted during uninstallation process.

Table 5.2.5 (1): Registry keys deleted.

Keys Deleted
• HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CurVer • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1 • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CLSID • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CurVer • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1 • HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\CLSID • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINPROGRESS • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINSYNC • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudNOSYNC • HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\pCloud Drive

Table 5.2.5 (2): Registry values deleted.

Values Deleted
• HKLM\SOFTWARE\Classes\CLSID\{063B8D8A-E610-3800-92BF-D2AF9DCDAB85}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{063B8D8A-E610-3800-92BF-D2AF9DCDAB85}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll" • HKLM\SOFTWARE\Classes\CLSID\{3103A792-C2D9-3C57-98DD-30071B26C05F}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll"

- HKLM\SOFTWARE\Classes\CLSID\{3103A792-C2D9-3C57-98DD-30071B26C05F}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\: "pCloudNOSYNC Class"
- HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\ProgID\: "OverlayIcon.pCloudNoSync.1"
- HKLM\SOFTWARE\Classes\CLSID\{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}\VersionIndependentProgID\: "OverlayIcon.pCloudNOSYNC"
- HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\: "pCloudINSYNC Class"
- HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\ProgID\: "OverlayIcon.pCloudINSYNC.1"
- HKLM\SOFTWARE\Classes\CLSID\{8D0C0582-552A-4A6B-9455-DA63E1F329C0}\VersionIndependentProgID\: "OverlayIcon.pCloudINSYNC"
- HKLM\SOFTWARE\Classes\CLSID\{A2D0C838-9DD7-35F6-A64B-0828607D8422}\InprocServer32\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{A2D0C838-9DD7-35F6-A64B-0828607D8422}\InprocServer32\3.10.1.0\CodeBase: "file:///C:/Program Files/pCloud Drive/ContextMenuHandler64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\: "pCloud_INPROGRESS Class"
- HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\InprocServer32\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\ProgID\: "OverlayIcon.pCloudInProgress.1"
- HKLM\SOFTWARE\Classes\CLSID\{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}\VersionIndependentProgID\: "OverlayIcon.pCloud_INPROGRESS"
- HKLM\SOFTWARE\Classes\Installer\Dependencies\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Dependencies\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Products\8A51FA49EEEB89D43B0DD7C705825BA3\ProductName: "pCloud Drive"
- HKLM\SOFTWARE\Classes\Installer\Products\8A51FA49EEEB89D43B0DD7C705825BA3\SourceList\PackageName: "pCloud Drive.msi"
- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon\: "pCloudINSYNC Class"

- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon\CurVer\: "OverlayIcon.pCloudINSYNC.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.MyOverlayIcon.1\: "pCloudINSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\: "pCloud_INPROGRESS Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CLSID\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress\CurVer\: "OverlayIcon.pCloudInProgress.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\: "pCloud_INPROGRESS Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudInProgress.1\CLSID\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\: "pCloudNOSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CLSID\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync\CurVer\: "OverlayIcon.pCloudNoSync.1"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\: "pCloudNOSYNC Class"
- HKLM\SOFTWARE\Classes\OverlayIcon.pCloudNoSync.1\CLSID\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"
- HKLM\SOFTWARE\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SOFTWARE\Classes\WOW6432Node\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\Classes\WOW6432Node\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINPROGRESS\: "{D8BFAFBD-B670-4252-9C17-9CF1C64C2BAF}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudINSYNC\: "{8D0C0582-552A-4A6B-9455-DA63E1F329C0}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ pCloudNOSYNC\: "{3858ED1B-8F1C-42ED-A8A9-FDBF591E3C6B}"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\: "1"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\de\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\es\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\fr\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\ja\: ""

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\nl\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\dbg\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\rls\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders\C:\Program Files\pCloud Drive\zh\: ""
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\17BCFBB5AC9A9BB4DA3F4B9C7E9331D8\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\ja\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\225192B6419CBBC4CAA1240908BE7170\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\pthreadVC2.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\410ECE1A32F741440B444504863D4ADD\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\pCloud.exe"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\584D9B900B1D5FB4B99BBE67C7738FDD\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\nl\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\83654B787874C4244B5733C954CE04EF\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\Microsoft\Windows\CurrentVersion\Run\pCloud"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8AA2B6BC4C59484558BCB8B828C5B0D8\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\pCloud\pCloud Drive\installed"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\9818DD341F2E62A4B9B65E9B1CA4496D\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\fr\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B8991F4234EFEBC4F8A2180B2B003A2C\8A51FA49EEEB89D43B0DD7C705825BA3: "21:\Software\pCloud\AppPath"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C007ED4F4337DDD47A7E6E2E0E4846BE\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\dbg\pSyncLib.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\DD1F3D05E323BE846819EE4D74518C8C\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\es\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\DE320DED86BA4A540901A6DBCE880357\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\"

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\E3444181A32776E4EB5F57153E4787A5\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\de\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\EC22AAA47CDD9B546A11C98BF67313CB\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\zh\ContextMenuHandler.resources.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F1439F25836095E469596EF5C547CAD5\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\ContextMenuHandler.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FDA3EC1B3490B5B409727AFB119AA409\8A51FA49EEEB89D43B0DD7C705825BA3: "C:\Program Files\pCloud Drive\rls\pSyncLib.dll"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8A51FA49EEEB89D43B0DD7C705825BA3\InstallProperties\Publisher: "pCloud AG"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8A51FA49EEEB89D43B0DD7C705825BA3\InstallProperties\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\Publisher: "pCloud AG"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{94AF15A8-BEEE-4D98-B3D0-7D7C5028B53A}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\BundleCachePath: "C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayIcon: "C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe,0"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\DisplayName: "pCloud Drive"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\Publisher: "pCloud AG"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\ModifyPath: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /modify"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\QuietUninstallString: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /uninstall /quiet"
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\UninstallString: ""C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe" /uninstall"

- HKLM\SOFTWARE\WOW6432Node\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\0\win64\: "C:\Program Files\pCloud Drive\OverlayIcon64.dll"
- HKLM\SOFTWARE\WOW6432Node\Classes\TypeLib\{ADF1FA2A-6EAA-4A97-A55F-3C8B92843EF5}\1.0\HELPDIR\: "C:\Program Files\pCloud Drive"
- HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{464388BE-BD94-4CD8-85F6-76264B687702}: "v2.30|Action=Allow|Active=TRUE|Dir=In|RA4=LocalSubnet|RA6=LocalSubnet|App=C:\Program Files\pCloud Drive\pCloud.exe|Name=PCloud AG|Edge=TRUE|"
- HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{464388BE-BD94-4CD8-85F6-76264B687702}: "v2.30|Action=Allow|Active=TRUE|Dir=In|RA4=LocalSubnet|RA6=LocalSubnet|App=C:\Program Files\pCloud Drive\pCloud.exe|Name=PCloud AG|Edge=TRUE|"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\pCloud Drive\installed: 0x00000001

Table 5.2.5 (3): Registry values added.

Values Added
• HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe: 07 99 0B 50 92 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 • HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe: 07 99 0B 50 92 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 • HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\ProgramData\Package Cache\{b64df1da-9ef1-4f19-8ba3-4a80618d12db}\pCloud Drive.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 B8 78 E2 00 9E 97 E2 00 03 00 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 50 BB 64 ED DD AC D5 01 00 00 00 00 00 00 00 02 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 CD 01 00 00 00 00 00 01 00 00 00 01 00 00 00

Table 5.2.5 (4): Registry Values Modified.

Values Modified
• HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program

Files\pCloud Drive\pCloud.exe: D9 DF 60 62 7E DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00

- HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program Files\pCloud Drive\pCloud.exe: 9E 49 A4 15 92 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program Files\pCloud Drive\pCloud.exe: D9 DF 60 62 7E DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1959509321-4289350582-1932700836-1001\\Device\HarddiskVolume2\Program Files\pCloud Drive\pCloud.exe: 9E 49 A4 15 92 DE D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\Logged: "True"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\Logged: ""
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\SyncDrive: "P:\"
- HKU\S-1-5-21-1959509321-4289350582-1932700836-1001\SOFTWARE\pCloud\SyncDrive: ""

To find any difference between registry added and deleted, in this case, all registry related to pCloud is collected into text file, separate it into two files; one for added registry and other for deleted registry. The texts were compared by using diffchecker.com.

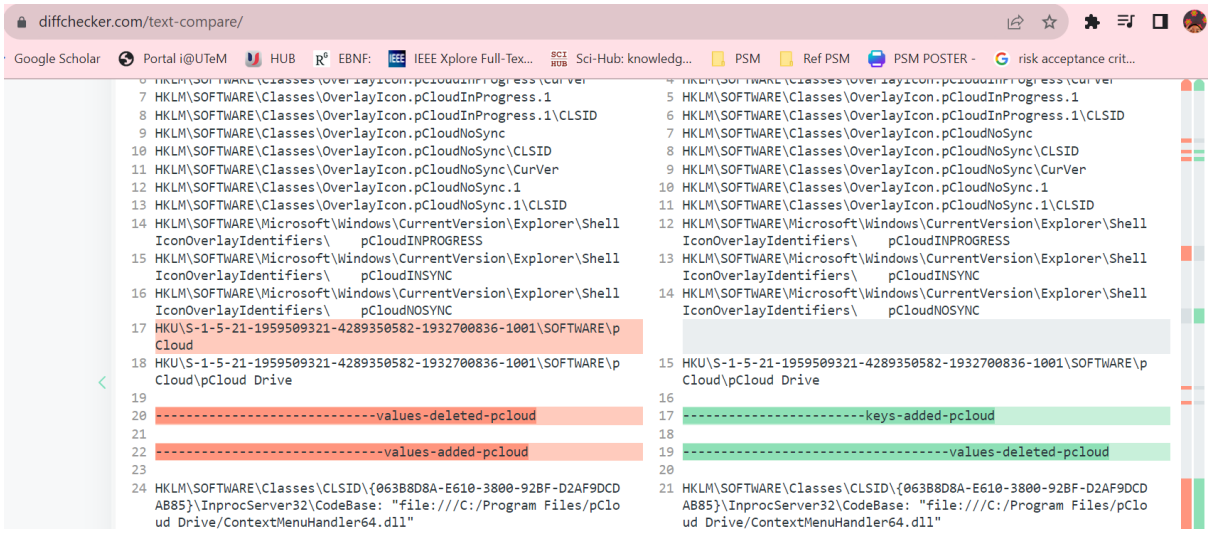


Figure 5.2.5: Comparison registry on diffchecker.com.

Based on **Figure 5.2.5** the right side is the registry added and the left side is the deleted file. As shown in the figure, the highlighted (red) registry that was added is not listed on the list of deleted registry. Thus, it shows that the highlighted registry remains in the monitor even after uninstallation of pCloud.

5.3 Keyword Formulation

In the keyword searching phase, keywords were collected through detailed examination of the virtual memory, akin to the computer's short-term memory. These chosen keywords were picked based on the investigation context.

Table 5.3 (1): Keyword formulation for Web Browser-Based Experiment

Keyword	**Content**
email=	Email (eg: pcloudfp@gmail.com)
email password	Password (eg: Pcloud_test0908)
"userid"	User ID
cookie=	Cookie
Pcauth=	
"currentfileuploaded"	File name that are currently uploaded
"currentfile"	
"name"	File name
"filename" (eg: "02.txt")	Content of file
"dwltag"	Metadata of downloaded file
modified	List of files in pCloud
deletefile	Deleted file URL of deleted file

Table 5.3 (2): Keyword formulation for Windows App-Based Experiment

Keyword	**Content**
username=	Username (eg: pcloudfp@gmail.com)
password=	Password (eg: Pcloud_test0908)
deviceid=	Device ID
pCloud	pCloud Directory
result	

metadata	Filename; for process upload, download and delete
created	
OpenFileContextData	
Filename (eg: testing_02)	Content of file
P:\	Location of Pcloud file

The results of the keywords are organized in Table and Table, serving as a guide to the investigation in the pCloud storage. This list includes many different words, some that are very specific to the case, and others that are more general phrases. These words are extremely valuable because they help to find important evidence in the cloud storage system as the investigation is continuing.

5.4 Summary of artifacts

After all experiments and analysis have been done on the Windows App-Based and Web Browser-Based, there are various kinds of artifacts can be retrieved.

Table 5.4: Summary of artifacts retrieved from this analysis.

Location	**Recovered Artifact**
Registry	Folder, Logfile, pCloud folder
Memory	Email, password, device id, user id, cookie, file name upload, file name download, content of pCloud, file content, metadata of file
Process	Folder, Logfile, pCloud folder
data.db file	Email, file uploaded, configuration, content of pCloud

Based on **Table 5.4**, it shows a rough summary of what artifacts can be retrieved from pCloud storage. This Table includes app-based and browser-based. Overall, many artifacts can be found in the memory. All this data can be retrieved using forensic tools that support memory analysis. From registry and process that are little artifacts can be extracted but it can lead to more artifact's discovery such as data.db file.

5.5 Guideline (Report)

Phase 1: Evidence source identification and preservation
1. Identify cloud storage service
2. Identify the process involve during incidents
3. Identify browser-based or app-based
4. Preserve the evidence in a manner consistent with forensic practices.

Phase 2: Collection
1. List specific data that want to be collected
2. Decide what software tools to use to gather the data
3. Ensure the data collected remain safe and unchanged
4. Compare the collected data with the original to check the data integrity
5. Keep the data safe

Phase 3: Keyword search
1. Make a list of relevant words or phrases related to the investigation
2. Decide tools to used that help in keyword searching
3. Understand the chosen tool feature for keyword searching, for example use regular expression or any special features for a better searching.
4. Decide on limits like dates or specific folders to narrow the searching to the most relevant data
5. Keep record the keyword and the limits of the searching
6. Make sure the data found related to the investigation as useful for evidence, not all data that match with the keyword are useful
7. Document the data found
8. If the first searches do not meet what important for the investigation, adjust your queries and try again.

Phase 4: Analysis
1. Review the results of data to find any important information related to the investigation

2. Take out the important data of the investigation
3. Analyze the data if there is any patterns or trends
4. Keep note how the analysis is done, what data found, what tools is used and what techniques is used
5. Explain how the findings relate the investigation's goals
6. Create a report on how the analysis is done

Phase 5: Reporting and presentation
1. Create a report that explains the investigation process and findings
2. Organize the report by dividing into logical sections, objectives, methodology, findings, and guideline
3. Keep report clear and concise
4. Use visuals (tables or graphs) to make findings easier to understand
5. Review the report with expert for feedback

Chapter 6: Conclusion

6.1 Conclusion

In summary, this research paper shows how investigating leftover traces in cloud storage and using keyword analysis can make digital investigations faster and more efficient. This is a significant improvement in the field of digital forensics, making it easier to find important information in cloud storage.

The impact of these findings on cloud users, they will know how much of there are being exposed while accessing cloud. Since user aware that some of their information are being exposed, they can decide whether is it okay to use the services and decide whether pCloud good for their privacy or not. This also mean any of their activities are trackable.

6.2 Future Work

Future work in this area should be concentrated on exploring more cloud storage services for the purpose of forensic analysis to improve forensic fields in future. Improve the investigation to get more in details on the analysis of cloud storage either the popular cloud storage services used now or the less known cloud storage.

REFERENCE

Dargahi, T., Dehghantanha, A. and Conti, M. (2017) 'Investigating storage as a service cloud platform', *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 185–204. doi:10.1016/b978-0-12-805303-4.00012-5.

Broberg, J. and Tari, Z. (2008) 'MetaCDN: Harnessing storage clouds for high performance content delivery', *Service-Oriented Computing – ICSOC 2007*, pp. 730–731. doi:10.1007/978-3-540-89652-4_67.

Rajan, R.A. (2012) 'Evolution of cloud storage as cloud computing infrastructure service', *IOSR Journal of Computer Engineering*, 1(1), pp. 38–45. doi:10.9790/0661-0113845.

Srikumar Venugopal, Scheduling Distributed Data-Intensive Applications on Global Grids, Doctoral diss., Department of Computer Science and Software Engineering, The University of Melbourne, Australia, July 2006.

Vaquero, L.M. *et al.* (2008a) 'A break in the clouds', *ACM SIGCOMM Computer Communication Review*, 39(1), pp. 50–55. doi:10.1145/1496091.1496100.

G.-U. Rehman, A. Ghani, S. Muhammad, M. Singh, and D. Singh, "elfishness in vehicular delay-tolerant networks," Sensors, vol. 20, no. 10, 2020

Arockiam, L. and Monikandan, S. (2014) 'Efficient cloud storage confidentiality to ensure data security', *2014 International Conference on Computer Communication and Informatics* [Preprint]. doi:10.1109/iccci.2014.6921762.

Kamara, S. and Lauter, K. (2010) 'Cryptographic cloud storage', *Financial Cryptography and Data Security*, pp. 136–149. doi:10.1007/978-3-642-14992-4_13.

Garg, H. and Dave, M. (2019) 'Securing IOT devices and securelyconnecting the dots using REST API and middleware', *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* [Preprint]. doi:10.1109/iot-siu.2019.8777334.

Jan, S.U. *et al.* (2020) 'Issues and challenges in Cloud Storage Architecture: A survey', *SSRN Electronic Journal* [Preprint]. doi:10.2139/ssrn.3630761.

Hutchings, A., Smith, R.G. and James, L. (2015) 'Criminals in the cloud: Crime, security threats, and prevention measures', *Cybercrime Risks and Responses*, pp. 146–162. doi:10.1057/9781137474162_10.

Breitinger, F., Zhang, X. and Quick, D. (2022) 'A forensic analysis of rclone and rclone's prospects for digital forensic investigations of Cloud Storage', *Forensic Science International: Digital Investigation*, 43, p. 301443. doi:10.1016/j.fsidi.2022.301443.

Luo, X. and Liao, Q. (2007) 'Awareness education as the key to ransomware prevention', *Information Systems Security*, 16(4), pp. 195–202. doi:10.1080/10658980701576412.

Baryamureeba V, Tushabe F. The enhanced digital investigation process model. In the Proceedings of the Fourth Digital Forensic Research Workshop. 2004.

Carrier B, Spafford EH. Getting physical with the digital investigation process. International Journal of Digital Evidence 2003; 2(2):1–20.

Kent, K. *et al.* (2006) *Guide to integrating forensic techniques into incident response* [Preprint]. doi:10.6028/nist.sp.800-86.

Hong Guo, Bo Jin and Ting Shang (2012) 'Forensic investigations in Cloud Environments', *2012 International Conference on Computer Science and Information Processing (CSIP)* [Preprint]. doi:10.1109/csip.2012.6308841.

Martini, B. and Choo, K.-K.R. (2012) 'An Integrated Conceptual Digital Forensic Framework for cloud computing', *Digital Investigation*, 9(2), pp. 71–80. doi:10.1016/j.diin.2012.07.001.

Simou, S. *et al.* (2016) 'A survey on cloud forensics challenges and solutions', *Security and Communication Networks*, 9(18), pp. 6285–6314. doi:10.1002/sec.1688.

Dargahi, T., Dehghantanha, A. and Conti, M. (2017a) 'Investigating storage as a service cloud platform', *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 185–204. doi:10.1016/b978-0-12-805303-4.00012-5.

Mohtasebi, S.H., Dehghantanha, A. and Choo, K.-K.R. (2017) 'Cloud storage forensics', *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 205–246. doi:10.1016/b978-0-12-805303-4.00013-7.

Dehghantanha, A. and Dargahi, T. (2017) 'Residual cloud forensics', *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 247–283. doi:10.1016/b978-0-12-805303-4.00014-9.

Hintea, D., Bird, R. and Green, M. (2017) 'An investigation into the forensic implications of the windows 10 operating system: Recoverable artefacts and significant changes from Windows 8.1', *International Journal of Electronic Security and Digital Forensics*, 9(4), p. 326. doi:10.1504/ijesdf.2017.087394.