International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. , No. (Mon-20..)

http://dx.doi.org/10.12785/ijcds/XXXXXX

Cloud Forensic Artifacts:
Digital Forensics Registry Artifacts discovered from Cloud Storage Application

Mohammed A. Bajahzar[1] and Prof. Shailendra Mishra[2]

[1]*College of Computer and Information Sciences, Majmaah University, Majmaah City, Saudi Arabia*
[2]*College of Computer and Information Sciences, Majmaah University, Majmaah City, Saudi Arabia*

Received Mon. 20, Revised Mon. 20, Accepted Mon. 20, Published Mon. 20

Abstract: Cloud storage drives have become very popular nowadays for many people around the world. Understanding how to locate, retrieve and acquire cloud-based data may be complex and time-consuming. Standard digital forensic concepts and thorough chain of custody methods are the main discussion topics in most contemporary academic forensic publications. The traditional approach to computer forensics emphasis physically accessing the media that houses the information that could be of factors that could contribute. On the other hand, while working in a cloud computing environment, accessing the physical media is practically not feasible. Data for a given client could be kept decentralized, spanning several data centers and countries, using various virtual servers and physical devices.

Due to the data breaches which can occur by cloud-based applications, this research proposed in this paper will focus on gathering evidence from Windows 11 operating systems to discover and collect left over registry artifacts by one of the main cloud storage applications known as OneDrive. Whereas it will imply their existence even after the unlinking and uninstalling of cloud drive applications. This proposed research will show what type of data remnants and where it can be found using the analysis of digital forensic investigator. Also, due to the time consuming to collect registry artifacts with their essential values, a bash script will be built to gather registry artifacts in which will show how data is stored within Windows 11 registry.

Moreover, there will be two main approaches for this research, the first approach will be taking a snapshot of Window's registry after the installation and linking account into the cloud storage application to perform digital forensic investigation on the machine to discover related artifacts in the registry. The second approach is to unlink account and uninstall OneDrive cloud drive applications as well as restarting the machine and then take another snapshot to perform a second forensic investigation to compare evidence gathered on the second approach with evidence gathered on the first approach.

Keywords: Digital Evidence, Cloud Forensic, Windows 11 Registry, Forensic artifacts, Cybersecurity

1. INTRODUCTION

As technology keeps developing, new cloud storage applications are introduced creating new challenges for digital forensic investigators as well as law enforcement [1]. Advanced cloud storage applications allow corporations and users to transfer, upload and save their data into the digital world. The increasing popularity of using cloud storage applications amongst individuals and users might increase the possibility of miss integrity of the data, which will construct user's concerns about their safety and privacy of important files and documents stored remotely.

The method involved in this proposed research is to identify, retrieve and analyze data from Windows 11 registry that may be provided as credible evidence in a legal proceeding which is referred to as digital forensics [2]. This discipline uses various approaches, techniques, and technologies to accomplish its goals. The data extraction procedure might be different for each device or kind of data being processed, depending on the situation's particulars. For instance, acquiring and analyzing data from a traditional computer's storage device necessitates a different method than gathering and analyzing data over a live network and is still another process for cloud-based technologies that incorporate evidence partition and dispersed settings [2]. No matter how the investigation is conducted, some forensic processes must be carried out extremely carefully to gather and save reliable digital information [2].

According to [3], in cloud forensics, there are no special techniques and there is a lack of knowledge as well as professionals who know how to use them. This is a problem, and it gets harder when data is encrypted, and loss of data control is involved. Establishing a cloud forensic capacity is

E-mail address: 431104384@s.mu.edu.sa, S.mishra@mu.edu.sa

a prerequisite for cloud companies and subscribers. If they do not, they will be susceptible to continuing issues while conducting a cloud forensic investigation, such as criminal invasions and serious policy breaches [3]. This is because they are more likely to face these challenges if cloud forensic capability is not built. Due to insufficient forensic expertise and preparation, investigators will also confront challenges when working with enforcement agencies in situations involving the confiscation of resources [3].

This proposal aims to examine and identify the registry artifacts gathered and retrieved during a cloud forensic investigation and evaluate the applicability and efficacy of the methodologies used to obtain the data within Windows 11 registry. The purpose of this research is to set up a scientific experiment that will show and compare how changes cloud storage applications can make to the registry within Windows 11. The experiment will be configured in such a way that it can be followed step-by-step and obtain the same results. This research project will also compile a summary of Windows registry artifacts caused using the cloud apps during installation and removal.

Specifically, this proposed research will concentrate on comparing the results between gathered data from cloud applications in two main approaches. Firstly, taking a snapshot of the registry without unlinking OneDrive application drive and analyze the gathered evidence to compare them with the second approach whereas the cloud storage application will be unlinked and removed from the machine and compare acquired evidence with first outcome.

A. Research Objectives

1) To study the literature related to registry artifacts related to cloud storage applications.
2) To understand the process and methodology used to obtain artifacts from cloud storage applications.
3) To discover cloud storage artifacts and perform forensic analysis discovering those artifacts.
4) To conduct Digital Forensic experiment to discover Windows 11 registry artifacts.
5) To identify all possible ways of retrieving digital evidence related to cloud computing in which it will minimize incident response timeline.

B. Research Challenges

1) Lack of time for expected delivery.
2) Expensive software license for cloud forensics.
3) The required intensive knowledge in digital forensic analysis skills.
4) Lack of academic resources related to digital forensics for cloud infrastructures.

C. Research Questions

1) What registry artifacts can be found when cloud applications are installed or uninstalled?
2) What is the process and methodology of obtaining artifacts of cloud storage applications when installed on Windows 11 Operating System?
3) How to discover forensic artifacts of cloud storage applications and how to perform forensic analysis discovering those artifacts?
4) How to identify all possible ways of retrieving digital evidence related to cloud computing in which it will minimize incident response timeline?

D. Statement of Problem

When conducting a digital forensic investigation, including the examination of registry files, investigators could run across a few significant challenges, including Data Completeness the kind of study and the quantity of information needed will determine how much information is needed. Certain inquiries call for the collection of more data than others. As a result, investigators need to ensure that all the data is there as well as comprehensive. If this is not the case, the inquiry can cost more money and take longer to conclude.

2. RELATED WORK-LITERATURE REVIEW

This section's primary research purpose is to evaluate the existing body of literature that is important to the subject domains, specifically referring to cloud computing technology as well as cloud digital forensics methodologies. The assessment of the work will help not only as a fact-finding exercise but also as a means of drawing attention to potential future issues and areas of study. MFIT lectures, supplementary readings, internet news sources, websites, journals, databases, and standard print reference books contributed to the student's understanding of the literary canon. This will cover the principles that govern the cloud, the many cloud models, and the services they provide, vitalized, multi-tenancy, cloud security issues, and so on. According to [4], Issues relating to governance, management, jurisdiction rights, confidentiality, and legal considerations. In conclusion, below is an outline of the procedure for collecting digital evidence in the case in a cloud environment [5].

A. Security Issues Within Cloud Computing

According to [6], which published the total number of records accessed was 12.3 billion. A single attack in 2019 was estimated to cost approximately 3,83,365 US Dollars. The entire number of significant data breaches that have been disclosed in 2019 is shown in Table 1. [6] has also stated that in 2019, 48% of firms recognize at least a single attack on a monthly basis, and 62% of organisations are capable of reacting rapidly to a data breach. At the end of 2019, an attack with ransomware occurred once every 30 seconds at an organization, and this rate is projected to increase to once every 11 seconds by 2021. In addition, corresponding to [6], from organizations in the year of 2019, almost 67% of organizations' systems have been reported as having been compromised. Also, only 31% of businesses have faced a cyber-attack on their own organizational infrastructure. These statistics were gathered from the reports of organizations in the year 2019. Unfortunately, only 50% of companies have not updated their protection

TABLE I. Data Breaches Numbers in 2019 [6]

Month	Total Breach	Data Record Breach
Jan	59	1.1 billion
Feb	58	870+ million
Mar	79	2.1 billion
Apr	71	1.3 billion
May	77	1.3 billion
Jun	64	39 million
Jul	92	2.3 billion
Aug	94	105 million
Sep	75	531 million
Oct	110	421 million
Nov	87	1.3 billion
Dec	90	627 million

strategy in more than three years. In 2019, phishing attacks accounted for 80% of all attacks; fraudulent email attacks accounted for 28% of all attacks; malware, ransomware, and spyware-related attacks are likely to account for 27%. These percentages are based on an analysis of different types of attacks. These percentages are according to research from the year 2019, which was published in 2019. Those who detect breaches on average every 197 days, whereas those who find breaches every 30 days save more than 1 million dollars in comparison to those that take 197 days.

According to the [7], there have been a total of 3,950 documented data breaches around the globe, and these incidents are still ongoing. The report provides a breakdown of each breach in terms of the industry and the service it affected. This analysis of the year 2020, spanning the period from the beginning of the year to the present day, found that simply 4% of data breaches included almost four and sometime more than 4 attackers performing actions and only 1% had associate players. The research of [7] covered the period from the beginning of the year to the current day. Organized criminal gangs were responsible for 55% of breaches. Internal actors were engaged in 30% of breaches. When victims are considered, it has been identified that 81% of security breaches were discovered within a week or fewer, 72% of security breaches featured victims from major businesses. However, 58% of victims had their personal data exposed. On the other hand, it is important to mention that there are more commonalities include 86% of data breaches being economically motivated, and 43% are using online applications, 37% stealing credentials such as usernames and passwords, 27% ransomware malware attacks, and finally, 22% of data breaches is attempted by phishing emails [7].

According to [8], Data Movement refers to data transportation from the client to the server and the opposite. As a result, there is a huge concern regarding data protection when data is in transit from the source to a specific destination.

a) Loss of Control

Protecting the data's privacy becomes the most critical issue as soon as it has been uploaded to a cloud storage service. This is because the cloud service provider or the personnel may improperly exploit the data for marketing purposes or for their own personal advantage [8].

b) Uncertain Performance

Since several users use the resources at the same time, there is a possibility that there may be problems associated with uncertain performance.

c) Identity Authentication & Unauthorized Access

As a result of the many different types of cyberattacks that are being carried out at the present time, it is extremely challenging to recognize and authenticate genuine users as opposed to false users or assailants.

d) Data Theft

Theft of data is a risk that may occur if cloud providers do not really keep up with the latest adequate storage compliance standards.

e) Denial of Service Attacks

If cloud providers cannot keep the minimum speed to develop their technology to identify and defend against cyberattacks, it is probable that denial of service assaults may occur [8].

f) Data Integrity

The integrity of the user's data is of the utmost importance, especially when cloud service providers modify user information [8].

However, Paper [9], have discussed various data encryption technologies. For instance, Searchable Encryption, Attribute-Based Encryption, Homomorphic Encryption and Identity Based Encryption in the context of cloud storages.

Moreover, Paper [9], have discussed various data encryption technologies. For instance, Attribute-Based Encryption, Identity Based Encryption, Searchable Encryption and Homomorphic Encryption in the context of cloud storages. However, [10] define threats as a "*potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allow an attack to be successful*". In other words, vulnerability is a flaw in a system that makes it possible for an attack to be successful. Nevertheless, presented threats in cloud computing field include data scavenging whereas device or memory destruction is required, account or service hijacking, DoS attacks, leakage of data, and 3rd party data manipulation, virtual machine escape, malicious virtual machine creation, insecure virtual machine migration and finally, sniffing or spoofing virtual networks. Virtual networks can be sniffed or spoofed in order to obtain sensitive information.

According to [11], problems with cloud storage include data integrity, data privacy as well as data recoverability and data backup. Cloud computing also faces challenges in terms of adequate media refinement. However, [12] suggests that a combination of symmetric key searchable encryption

and encrypted deduplication remains open research issues that require further investigation and analysis in the cloud security field.

B. Cloud Storage Application Providers

One of the most popular uses of cloud computing these days is for off-site data storage, which may be accomplished via many methods [13]. Regardless of the size of their company, cloud storage users absolutely cannot overlook the need for security. An application for cloud computing storage must retain high speed and maximum scalability while also providing highly accessible access to the data being stored. In addition, the accuracy of the data must be verified, and dependability is of the highest significance in an application that stores data [13]. Typically, a kind of cryptography is used as a security measure, but the location and timing of its application are crucial. At the very least, the client's data must be safe and uncorrupted while it is stored on the cloud. The cloud provider that hosts the client's data is the one who is responsible for providing access to the data. However, unauthorized users are unable to view or modify the data [14].

Furthermore, Users are able to adjust cloud data storage to fit their requirements since it provides access to a large pool of shared resources. Users are provided with storage service through cloud storage, which is achieved by the utilization of application clusters, web technologies, and distributed file systems to bring together various types of storage devices. It is important to mention some of cloud service providers such as OneDrive, Azure, GoogleDrive, Alibaba and IBM cloud are one of the well-known cloud storage applications that offer a variety of security options to protect user's data as well as user privacy [14].

Also, [14] indicate that the most important cloud security measures that major cloud providers offer as a part of their cloud services which will be outlined in Table 2 to facilitate a deeper level of comprehension. Based on the comparison in Table 2, it has been identified that if the circumstances require calls for the management of all important security controls, OneDrive may be given high priority. After OneDrive, the use of GoogleDrive should be considered a high priority if there is a possibility that an issue would arise regarding the safety of any reputable organization's email communications [14]. When managing cloud application services, such as recovery and backup, change management, vulnerability assessment and patch management should be prioritized within an organizational environment. Any of the above cloud providers may be a good fit for any organisations when the following security controls are well implemented. For instance, multi-factor authentication, DDoS protection, internal and external firewall, key management, encryption at rest and identity access management [14].

C. Computer Forensics: Digital Forensic Methodology

Compared to other branches of forensic science, the field of computer forensics is regarded as being one of the more recent ones to have emerged. Unfortunately, huge numbers of people do not actually realize what the term "computer forensics" refers to or the processes that are engaged [15]. There is a lack of comprehension of the distinction that may be made between the data extraction and the data analysis procedure. In addition, there is a dearth of understanding these two processes' functions in the overall forensic process. Therefore, it is important to note that the cybercrime lab is a part of the computer forensics and Intellectual Property Section (CCIPS), whereas a has been developed a flowchart detailing the steps involved in conducting a digital forensic analysis. In this research, the flowchart serves as an illustrative help for explaining the approach and its actions.

TABLE II. Important Cloud Storage Security Controls [14]

Security Control	OneDrive	Azure	Alibaba	IBM
Firewalls	✓	✓	✓	✓
SIEM	✓	✓	✓	✓
Anti-Malware	3rd Party	✓	✓	3rd Party
Data Loss Prevention	✓	✓	✓	3rd Party
File Integrity Management	3rd Party	✓	3rd Party	3rd Party
Encryption	✓	✓	✓	✓
Endpoint Protection	3rd Party	3rd Party	✓	3rd Party
Identity Access Management	✓	✓	✓	✓
Backups & Recovery	✓	✓	✓	✓
Change Management	3rd Party	✓	✓	3rd Party
Patch Management	3rd Party	✓	3rd Party	✓
Multi-factor Authentication	✓	✓	✓	✓

The following is a comprehensive definition of computer forensics: the application of scientifically developed and proven approaches towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence generated from digital sources with the aim of aiding or promoting the reconstruction of events judged to be illegal. These methods are used to validate, collect, analyze, identify, document, interpret and present digital evidence produced from digital sources or devices [15]. The following the key components of computer forensic examinations:

- Obtaining & Imaging Forensic Data.
- Fill in a Forensic Request (Chain of Custody Form) for Validations
- Preparation & Extraction.
- Identification.
- Analysis & interpretation.
- Forensic Report & Presentation.

Businesses could delegate those tasks to many teams or departments in day-to-day operations. Even if this is not only permissible but also sometimes essential, the fact that it may lead to confusion and dissatisfaction should not be overlooked. The various law enforcement authorities

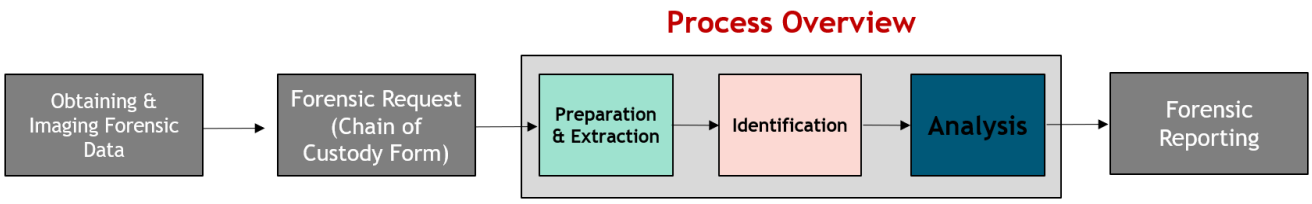

Figure 1. Digital Forensic Process [15]

need to have transparent lines of communication if they are to collaborate successfully. During conducting their investigation, the team must remain mindful of the wider picture while still being specific when referring to the many aspects of the problem.

The prosecutor and the forensic examiner are the ones who are responsible for determining then the procedure must be finished at each phase of any investigation or prosecution. and then communicate their decisions to each other [15]. Since the process may include iteration, they are required to choose the appropriate number of times to carry out the procedure, everyone needs to know whether a case just requires collection, extraction preparation, validation, and identification of evidence or whether it also demands analysis [15].

Examiners go on to the next three steps of the method after first acquiring forensic data and a request, each of which is described in more detail in the following section of this research. Nevertheless, these three procedures are not finished until case-level analysis and reporting are conducted. Examiners try to be clear about each individual procedure that is included in the methodology. Depending on the specifics of the case, examiners may choose to condense some steps of the process or combine certain steps altogether [15]. When examiners refer to the lists in this fashion, they are not trying to convey the appearance that the lists, such as the "Relevant Data List," are genuine written documents as they are doing so. It is possible to write the lists, or one may just commit the entries to memory. In conclusion, keep in mind that investigators often go through this whole procedure again since a discovery or conclusion may point to new leads that needed to be investigated [4].

D. Related Articles & Cybersecurity Majors: (Need Update)

3. METHODOLOGY

The used methodology of this research involves a practical simulation of registry artifacts collections whereas a study of all possible changes of registry will be monitored and tracked while the installation and removal of OneDrive cloud application. Thos, a bash script will be implemented to improve the collection of registry values and artifacts in which is related to cloud storage application.

The design of a research topic and the development of a suitable technique and structure for the proposed study is the fundamental purpose of the research. For researchers and investors, the dispersed nature of data in cloud technology, the architectural functionality of virtualization, and the limited physical accessibility to server-side digital evidence are genuine obstacles. In these cases, standard procedures for evidence gathering and restoration may not apply, and as a result, they may not be able to withstand examination in a legal setting.

This presents research papers on digital forensics in the cloud to examine the applicability of traditional digital forensics tools and methodologies to cloud forensic investigations and the trustworthiness and integrity of the data gathered to get knowledge from research and experiences that are comparable to those undertaken by other scientists who are working in the same area. In addition, a few references that might help speed up conducting forensic inquiry in a public cloud. The research papers were chosen because of their relevance and resemblance to the chosen study field. This similarity includes the technique that was employed as well as significant material that pertains to cloud digital forensic investigations.

The first investigation, which was conducted by [15], demonstrates that it is feasible to uncover evidence concerning the interaction between the User and the CSP by exploring local artifacts. The second study, conducted by [13], provides an overview of the field of forensics in the context of a cloud-based distributed file system. A detailed forensic analysis of tackles technical and procedural problems is included in this investigation. The findings of the digital forensic tests conducted by [14], in their third experiment to get a comprehensive knowledge of the artifacts required to execute cloud storage forensics are of tremendous use to forensic practitioners and researchers (SaaS).

The figure (2) simply implies the steps followed to implement the research methodology to conduct practical experiments. Furthermore, explaining the above figure can be shown below:

- **Grey Boxes** - Represent the beginning and ending steps of the methodology.
- **Yellow Boxes** - Represent the first approach of the methodology whereas a snapshot of the registry will

TABLE III. Discovered Artifacts After Removing OneDrive

Cite Key	Security	Threat & Attacks	Detection & Mitigation	Incident Response	Standards & Policy	Important Findings
[1]	✓	-	✓	✓	-	Cybersecurity blog put a strong emphasis on identifying Uncommon Event Log Analysis for Incident Response and Forensic Investigations techniques.
[2]	✓	✓	✓	✓	✓	The workshop book includes the digital forensic investigation process and digital forensic analysis of digital devices. Following the proposed process will result accurate acquisition of digital data.
[3]	✓	✓	✓	✓	-	How cloud computing can be secured and what are the main concerns which should be addressed when implementing cloud computing as an infrastructure.
[16]	✓	✓	-	✓	✓	A detailed analysis of several cloud computing challenges in the digital forensic world.
[4]	✓	-	✓	✓	✓	NIST Cloud Computing Standards Roadmap where best practices approach is presented to conduct forensically sound digital investigation
[5]	✓	✓	-	-	-	Types of cloud computing and how it is actually works in the cybersecurity world and what is the main impacts and issues faced by organizations.
[6]	✓	✓	✓	-	-	How private and secure is the cloud computing and what value can be added to organization securing their environment using cloud computing.
[7]	✓	✓	-	✓	✓	The Problem with Cloud-Computing Standardization and how can be solved and addressed.
[8]	✓	-	-	✓	-	Engaging Trustable Hypervisor Log Evidence Within a Cloud Forensic Environment
[9]	✓	✓	-	✓	-	How Security, privacy and forensic issues are the primary obstacles in the growth of cloud computing systems
[10]	✓	✓	✓	✓	✓	forensic investigation on cloud storage application research
[11]	✓	✓	✓	✓	✓	Forensic investigation was conducted on logs using forensic server.
[12]	✓	-	✓	-	✓	Digital forensic approach for investigation of cybercrimes in private cloud environment
[13]	✓	✓	✓	-	✓	Challenges in cloud computing when performing digital forensic investigation.
[14]	✓	✓	-	✓	✓	How to forensically handle security incidents during the investigation of digital devices.
[15]	✓	-	✓	✓	✓	Step by step guidelines in digital forensics processes.

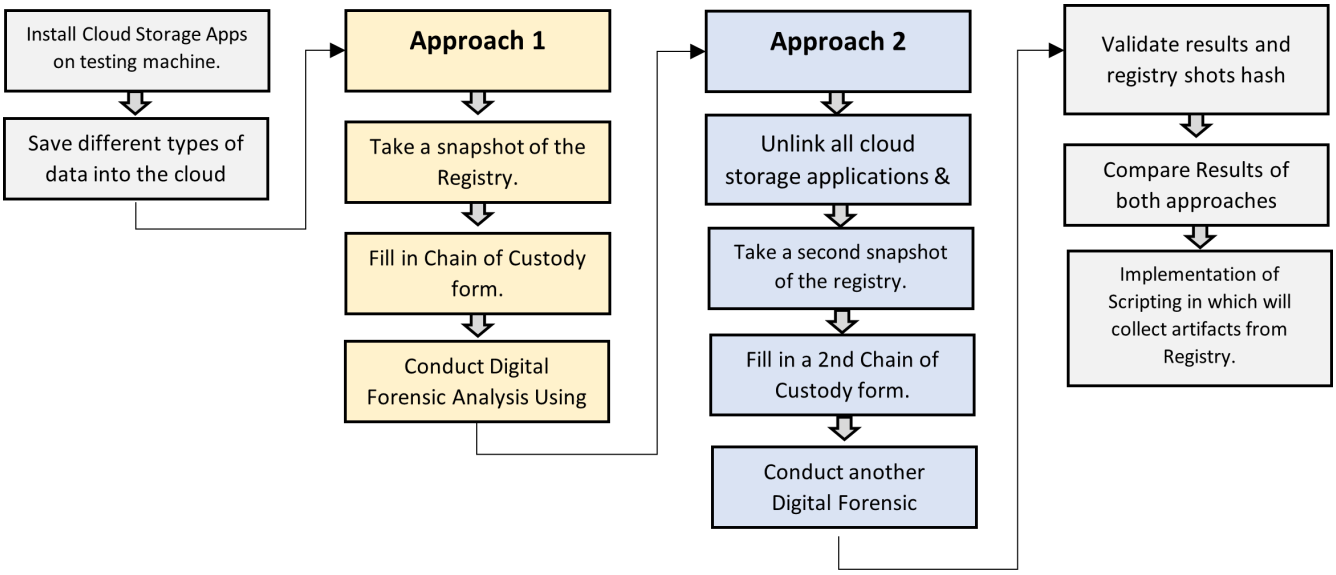

Figure 2. Research Methodology

be taken to gather artifacts and possible and retrieval artifacts.

- **Blue Boxes** - Represent the second approach whereas unlinking and restarting the system to take a second registry snapshot.

In addition, below are the main objectives of the methodology used in this proposed project:

- To analyze literature related to registry artifacts of cloud storage applications.
- Various cybersecurity issues and problems for cloud computing systems.
- Various digital forensic techniques/technologies/methodologies retrieve and discover forensic artifacts in windows registry.
- The environment used for gathering cloud artifacts would be identified.
- To develop a digital forensic technique in discovering forensic artifacts when investigating data on cloud storage applications.
- Various techniques and tools will be used to perform required experiments.
- To compare achieved results gathered from the first approach and the second approach.
- Comparing results will allow us to provide justifiable reasoning for differentiating results or similar results.

A. Research Question and Hypothesis

- **Main Research Question**: When performing a digital forensic investigation on Windows 11 registry based on cloud storage applications, what type of artifacts can be collected and gathered?
- **Research Question 2**: How are registry artifacts related to cloud applications when installed?
- **Research Question 3**: What is the process and methodology of cloud storage applications when installed on Windows 11 Operating System?
- **Research Question 4**: How to discover forensic artifacts of cloud storage applications and how to perform forensic analysis discovering those artifacts?
- **Research Question 5**: How to identify all possible ways of retrieving digital evidence related to cloud computing in which it will minimize incident response timeline.
- **Asserted Main Hypothesis**: Forensic artifacts can be found and seen when analyzing windows registry.
- **Hypothesis 1**: Both snapshots of registry should illustrate different outputs (results).
- **Hypothesis 2**: Forensic artifacts should be discovered after the unlinking the cloud storage applications.

B. Proposed Scenario for System Modeling

The figure (3) contains the proposed scenario whereas the suggested system Modeling can possibly be used as a solution which will collect all gathered registry artifacts of OneDrive application. It is important to explain each step

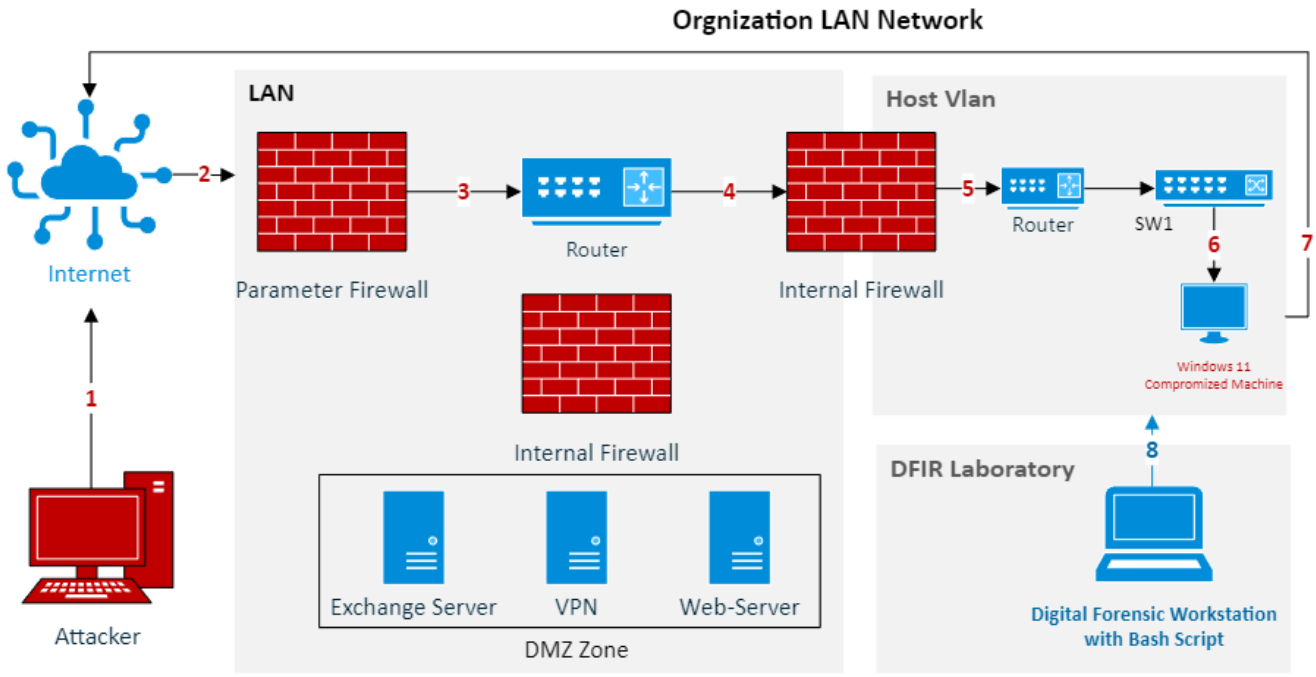

Figure 3. Proposed Scenario for System Modeling usage

within the proposed system in order to ensure how it works and to measure its effectiveness on below steps:

1) Attacker will establish an Internet Connection.
2) The attacker will then initiate access to the organizational internal network.
3) The attacker has successfully passed the parameter firewall.
4) The attacker has determined the routing table and know the host Vlan
5) The internal firewall was successfully passed.
6) Windows 11 system has been compromised and the attacker OneDrive account has been linked to the compromised machine to leak organization data.
7) Attacker started to upload data into the OneDrive storage.
8) With the help of the Digital forensic Lab and implemented scripts, registry artifacts have been collected to take advantage of left over artifacts or leads to know the identity of the attacker.

C. System Modeling Architecture

It is important to mention that the suggested system modelling architecture will help to collect all related artifacts which will be discovered during the practical experiment. The below figure indicate how exactly will the system work since the start of establishing connection from the digital forensic machine till the result gathering for analysis:

1) Digital Forensic workstation will establish a secure remote connection with the infected machine on the host Vlan.

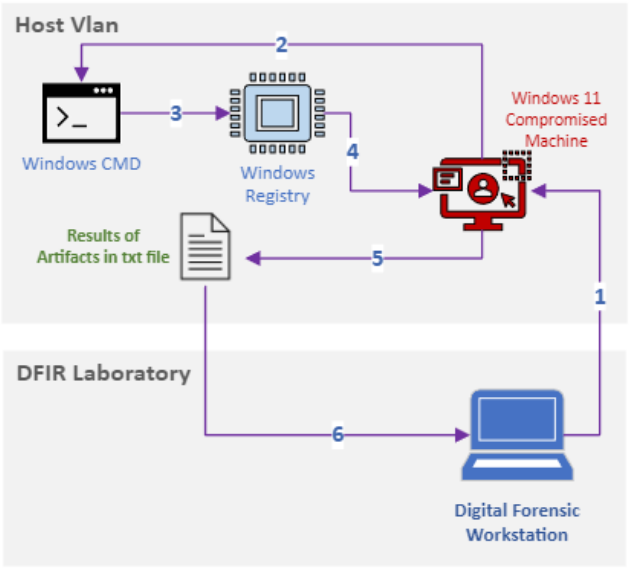

Figure 4. System Modeling Architecture

2) The suggested bash script will be copied into the infected machine to be run as an administrator.
3) The script will use Windows CMD terminal to run the bash script as Windows admin.
4) The CMD terminal will request queries from the Windows registry of infected machine to collect all required artifacts related to OneDrive application.
5) All observed artifacts will be saved into a text file

containing the identified keys and values of Windows registry.

6) Gathered results will be sent to the digital forensic workstation for hash validation and further forensic analysis and reporting.

4. EXPERIMENTAL SETUPS & ANALYSIS

A. Practical Environment Requirements

1) Using VMware Workstation V16.0.0, this experiment will be conducted.
2) Windows 11 (64-bit) will freshly be installed of with the following configurations:
   a) 30 GB of hard disk.
   b) 4 GB of memory.
   c) Guest OS will be allocated with 8 processors.
   d) Time zone was adjusted to +3GMT (Saudi Arabia) after the first boot-up, and Windows update was disabled to avoid any adjustments to the Windows registry.
   e) Google Chrome (v17.0) was installed on the Virtual Machine to be used to install Regshot application (v1.9.7) and 7Zip (v24.5) to keep track of the changes in Windows 11 registry.
   f) A total of two snapshots will be taken before and after the linking and unlinking the OneDrive Application.

B. Practical Procedures

This experiment is based on OneDrive artifacts produced by Windows registry. However, the focus of this practical simulation is primarily on the monitoring of the changes that occurred on Windows registry. OneDrive was linked to an official Majmaah University account, files were uploaded, and account was unlinked, and OneDrive application was uninstalled from Windows 11 to analyze left over artifacts. The way that OneDrive application interact and behave with the Windows registry can be predicted by referring to Windows registry analysis research and books. This possibly will give hints for the predictable results in a certain registry entry. However, all harmful software including malware will likely behave similarly and visually.

Regshot was used to take two snapshots and compare between them in term of the following instances:

a) After Linking OneDrive to an account and upload evidence items.
b) After unlinking and uninstalling OneDrive

However, the analysis stage covered the elements below:

1) Export certain keys into a txt file
2) Identify the Last Write Time.
3) Manually explore predictable forensic artifacts on the registry.
4) Keywords search via snapshot result.

C. Experiment's Life Cycle

Below process graph suggest the life cycle which was followed to complete the experiment.

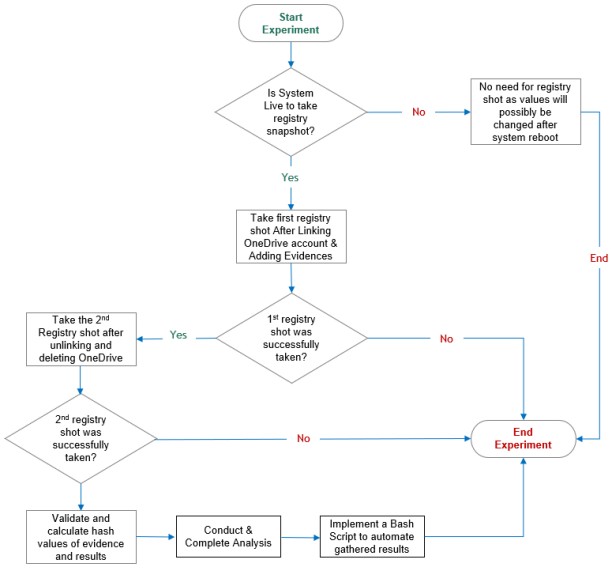

Figure 5. Experiment Life Cycle

D. Implemented Script

The implemented script in table (IV) was conducted because of this experiment whereas registry key, values and artifacts can be manually collected via the Command Prompt and all identified results will be saved on a txt file named RegistryCollecterResults.txt

5. RESULTS & ANALYSIS

Since linking, unlinking, and removing OneDrive application on the virtual system resulted in the discovery of Windows registry artifacts. Since there are no easy lists of values or keys that might provide all the answers, the results are evaluated using the earlier mentioned method to discover related artifacts. This part provides a list of raw findings, along with their values from a forensics perspective and further extensive analysis of all identified forensics artefacts on the subsections below.

A. Discovered Artifacts After Unlinking & Removing OneDrive

It is important to note that after unlinking and uninstalling OneDrive storage application from the targeted VM, there were some of the artifacts which were left behind and can be used as a trace of evidence during any digital forensic investigation. All identified and discovered artifacts can be shown in table (V):

OneDrive network states cache SSO was one of the artifacts which was left behind after unlinking the *OneDrive* application from the associated account. This can help to determine if any account is still connected or associated within *OneDrive* account.

TABLE IV. Discovered Artifacts After Removing OneDrive

Implemented Script Functionality	
Command Line Script	**Explanation of Script Action**
`start %windir%\system32\cmd.exe`	To start off the CMD.
Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive" /v "UserNameCollection" > C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for Username from registry in which is related to OneDrive.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive" /v "UserDomainCollection" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for User Domain from registry in which is related to OneDrive.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive" /v "HostNameCollection" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for Hostname from registry in which is related to OneDrive.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "UserEmail" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for User Email Address from registry in which is related to OneDrive
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "UserFolder" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for User folder from registry in which is related to OneDrive.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive" /v "Version" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for OneDrive Version from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\23.048.0305.0002" /v "InstallPaths" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for OneDrive installation path from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "DisplayName" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for OneDrive Display name from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "FirstRunSignInOriginDateTime" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for the first date & time of OneDrive first time sign in from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "WebView2InstallCheckedTimeStamp" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for the first date & time of OneDrive installation from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "LastSignInTime" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for the last date & time of OneDrive sign from registry.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1" /v "LastKnownCloudFilesEnabled" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for last known cloud files which were uploaded into OneDrive cloud.
& Reg Query "HKEY_USERS\S-1-12-1-2867766423-1316984426-2432438189-2443756634 \Software\Microsoft\Windows\CurrentVersion\Uninstall" >> C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for any uninstallation action of OneDrive cloud.
& Reg Query "HKEY_CURRENT_USER\Software\Microsoft\OneDrive" /v "UserInitiatedUninstall" ≫ C:\Users\431104384\Desktop\RegistryCollectorResults.txt	Request for user initiation of uninstallation of OneDrive cloud.

TABLE V. Discovered Artifacts After Removing OneDrive

Sub-Keys	Key Locations
OneDrive Network states cache SSO	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{78DE489B-7931-4f14-83B4-C56D38AC9FFA}
OneDrive App ID	\HKEY_CLASSES_ROOT\AppID\OneDrive.EXE “AppID” = {EEABD3A3-784D-4334-AAFC-BB13234F17CF}
OneDrive Update Failed Reason	\HKEY_CURRENT_USER\Software\Microsoft\OneDrive\UpdateFailedReason
Uninstallation of OneDrive	HKU\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Software\Microsoft\Windows\CurrentVersion\Uninstall\OneDriveSetup.exe
OneDrive Deleted Directory	HKU\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Software\Microsoft\OneDrive\DeletedDirectories

OneDrive App ID is a discovered artifacts which was left behind after the uninstallation of the *OneDrive* application. This can help the investigator to identify the application ID and discover any related evidence to it.

In addition, *OneDrive* uninstallation shows the directory where a registry key value can be saved when removing *OneDrive* app has been launched. Also, after uninstalling *OneDrive*, a deleted directory was created under the account directory which also indicate a deletion of *OneDrive* Application

B. Configuration Settings Artifacts

As part of the analysis, the configuration settings artifacts have been revealed in which it is helpful for investigator to determine the locations of *OneDrive* storage application:

1) Silent business configuration was successfully completed, this indicate the *OneDrive* application has been connected to a business account. This can be discovered from below registry path:
HKEY_CURRENT_USER\Software\Microsoft\OneDrive\SilentBusinessConfigCompleted

2) The installation path for the OneDrive application was on the following path:

Users\431104384\AppData\Local\Microsoft\OneDrive\23.043.0226.0001

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\23.043.0226.0001\InstallPath

3) The installed version of OneDrive was discovered as version 23.043. This artifact was discovered from below registry path:

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Version

4) Once unlinking OneDrive account has been initiated, OneDrive Icon has been changed from available and colourful icon to grey unavailable icon As. This indicate OneDrive account has been signed off and it is needed to sign on again to sync (Refer to figure 25).

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\HasSystrayIconBeenPromoted

5) User Initiated uninstall of the OneDrive cloud storage application from the VM. This was discovered during the analysis of below registry key:

HKEY_CUR0RENT_USER\Software\Microsoft\OneDrive\UserInitiatedUninstall

C. Associated User Account Related Artifacts

1) The associated user email address which was discovered as an artifact is “**431104384@s.mu.edu.sa**”. This can be identified from below registry key:

HKEY_USERS\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Software\Microsoft\OneDrive\Accounts\Business1

2) User domain collection associated with login account to Windows is shown as “**Majstudent**” Which is related to Majmaah university domain associated with Microsoft services. This was discovered during the analysis of below registry key:

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\UserDomainCollection0

3) Host name of the collection VM was discovered as “**mohammed**”. This is helpful as one of the identified artifacts which was revealed and pointing at the username associated within the used VM. This can be discovered from below registry key:

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\HostNameCollection

D. Timeline Related Artifacts

OneDrive application is using the following user account which is related to the experimental Windows account: "**431104384**". And its saved location can be found on the following:
`C:\Users\431104384\AppData\Local\Microsoft\OneDrive`

E. Artifacts that reveal details of a directory

1) Identified directory was pointing directly to the installation directory of OneDrive.

   `HKU\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Environment\OneDriveCommercial: "C:\Users\431104384\OneDrive - Majma'ah University"`

2) Another discovered artifact was the target folder path which all evidence items were saved into:

   `C:\Users\431104384\OneDrive` - Majma'ah University

   This will help investigators when trying to recover saved artifacts on local hard disk drives. This was discovered from the below registry key path:

   `HKEY_CLASSES_ROOT\CLSID\{04271989-C4D2-9335-754B-44D063EF5406}\Instance\InitPropertyBag\TargetFolderPath`

3) Business account was pointing at Majmaah SharePoint. This is helpful as it is indicating the associated account was commercial account and it is pointing to the associated business where it could be counted as a lead for further evidence gathering. This can be identified from below registry key path:

   `HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1\SPOResourceId\https://majmaah-my.sharepoint.com/`

F. Result Comparisons

1) Comparing between 1st & 2nd Registry Shot

As discussed in research methodology, there will be a comparison of registry shots gathered during the conduction of this experiment. The first comparison contains the registry shot which was taken after signing into *OneDrive* and uploading evidence items. The second registry shot was taken after successfully unlinking and uninstalling *OneDrive* Completely from the VM. Below table contain the differences between both registries in terms of the keys and values.

G. Script Results

Below table indicates the results which will be collected by the script that was explained in the section 4.4 Implemented Script. The script will help investigators in their analysis during a data breach investigation and will save their time and effort once registry investigation is required, instead of checking each registry hive, keys, and values one by one, the script will collect all relevant artifacts to OneDrive application and represent it in a .txt file as an output.

6. DISCUSSIONS

This discussion chapter on digital forensics on cloud-based applications, the registry keys finding may be a lead which can be used to detect if there was a breach of data using cloud drives. This chapter will also summarize the discovered and identified findings from the previous chapter and offer a development solution for the reason of collecting all discovered artifacts within the Windows registry in which is related to cloud drive forensic.

A. Key Findings & Observations

As OneDrive application is pre-installed on all Windows 11 workstations, there are some registry artifacts which already exist with windows default registry settings. However, during the linking, unlinking, and removing OneDrive application there were many different keys and values added, deleted, and modified in the Window's registry. For instance, OneDrive setting artifacts, OneDrive configuration settings artifacts, OneDrive associated user artifacts and finally, timeline related artifacts.

Initially, for Linking account artifacts, there was a file launch registry value observed which indicate there is a use of OneDrive Application. In addition, OneDrive updates was triggered and detected via the registry which means that OneDrive application was looking for last updated version since it was linked to a user. All results were mentioned in section 5.1 and results were displayed in Table 2: Discovered Artifacts After Linking OneDrive.

Secondly, after unlinking and uninstalling OneDrive from the application list, there were artifacts occurred on Windows registry such as OneDrive network states cache SSO which was indicating that there is no account associated with the current OneDrive. Also, OneDrive updated failed key was added as OneDrive was not able to get an update for an account to upload files or docs. Because of removing the OneDrive app, uninstallation key of OneDrive was added as well as a OneDrive deleted directory was initiated in the registry. All mentioned artifacts are indications of unlinking and uninstalling of the OneDrive application. All discovered findings can be found on section 5.2, Table: 3 Discovered Artifacts After Unlinking & Uninstalling OneDrive.

Thirdly, the configuration settings artifacts have been revealed in which it contains configuration artifacts for both approaches which can possibly be helpful for investigator to determine the locations path and folder for OneDrive storage application and the post authentication conditions has been discovered having the value 1 which indicate there was a successful authentication for the business account

TABLE VI. Timeline Artifacts

Description	Timeline Artifacts	Registry Values
The First Run Sign In Origin Date Time was identified	**Data Value in Hex:** 64132543 **Data Value in Decimals:** 1678976323 **Convert Decimals to time zone:** Thursday March 16, 2023, 17:18:43	HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1\FirstRunSignInOriginDateTime\1678976323
Installation Time Checked of OneDrive	**Data Value in Hex:** 6413253d **Data Value in Decimals:** 1678976317 **Convert Decimals to time zone:** Thursday March 16, 2023, 17:18:37	HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1\WebView2InstallCheckedTimeStamp\1678976317
Last update of the OneDrive Folder	**Data Value in Hex:** 64134692 **Data Value in Decimals:** 1678984850 **Convert Decimals to time zone:** Thursday March 16, 2023, 19:40:50	HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\LastUpdate\1678984850
Last Sign in Time into OneDrive	**Data Value in Hex:** 64132549 **Data Value in Decimals:** 1678976329 **Convert Decimals to time zone:** Thursday March 16, 2023, 17:18:49	HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1\LastSignInTime\1678976329

TABLE VII. Result Comparison of Both Registry Shots

Comparison between first and second registry shots		
Registry Changes	**Meanings**	**Explanation of Result**
72574 Keys deleted	According to [3] registry keys are "containers objects in which is similar to folders." Keys in registry may contain subkeys and values.	Key deleted suggest the number of deleted keys that were found missing from the first registry shoot and the second registry shot. Deleted keys occurred due to disabling windows updates as well as isolating the VM from any external connections.
249840 Values deleted	In registry, values hold certain instructions that applications in windows will refer to [16].	Deleted values will most likely be that values in which was associated within the deleted key above.
2544 Values added		This indicates the total number of added and modified values due to the installation of the cloud applications as well as linking both applications into a specific account and uploading evidence items into both applications.
445 Values modified		
326745 Total No of Changes	All changes occurred between the 2 registry shots including the deleted keys and value as well as added and modified values.	

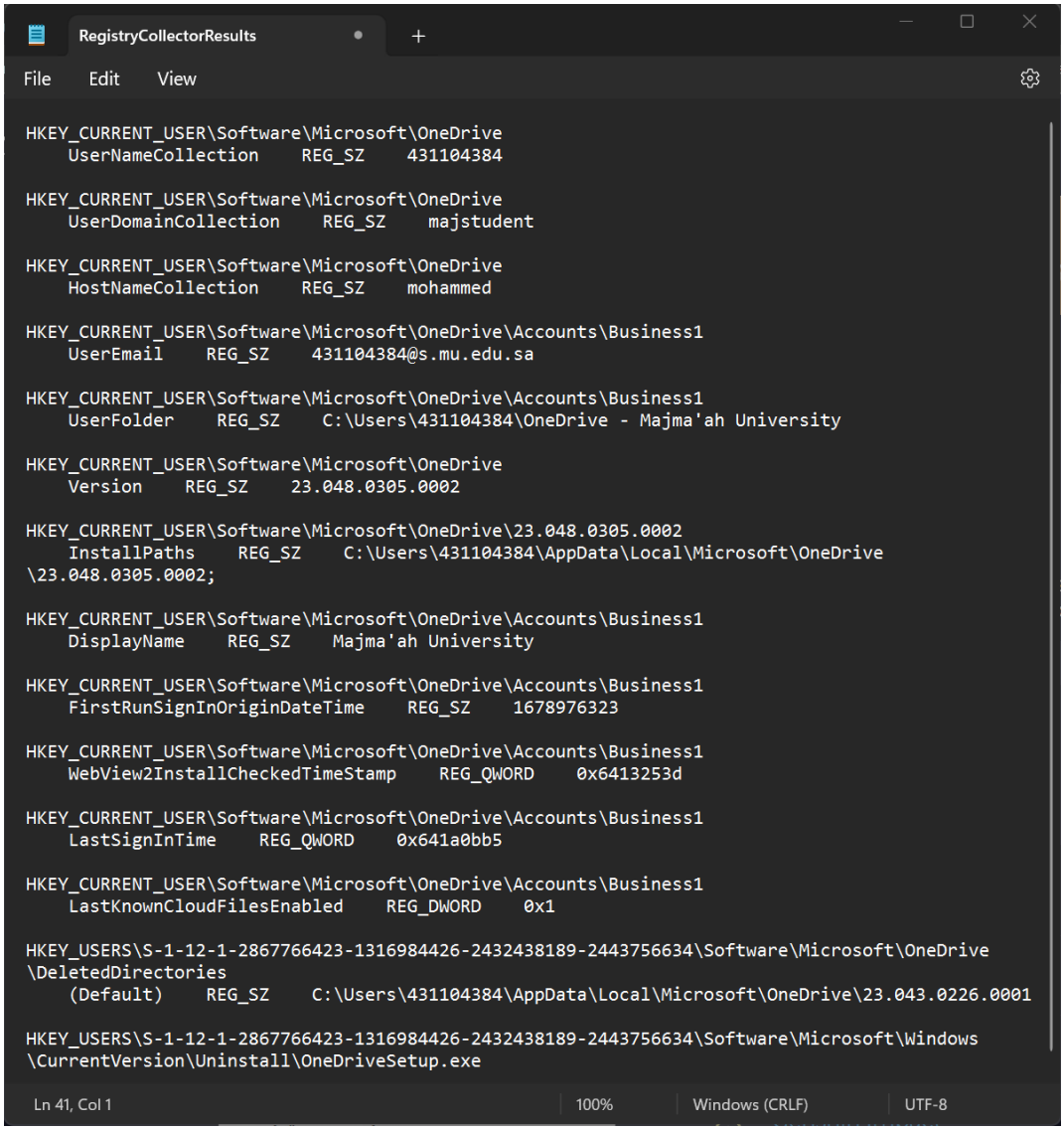

Figure 6. Script Collected Results in text file

on OneDrive as well as the installed version of OneDrive. Moreover, the last migration folder is indicating the value of 1, this means it is true that the files uploaded from the cloud was including: pictures, Screenshots, Desktops. However, Once unlinking OneDrive account has been initiated, OneDrive Icon has been changed from available and colorful icon to grey unavailable icon As. This indicate OneDrive account has been signed off and it is needed to sign on again to sync.

Fourthly, associated user configuration settings were also revealed. For example, the Username Collection which was pointing to 431104384@s.mu.edu.sa. Which is the account that was used to sign into OneDrive. Furthermore, User domain collection associated with login account to Windows is shown as "**Majstudent**" Which is related to Majmaah University domain associated with Microsoft services. Finally, Hostname of the collection VM was discovered. This is helpful as one of the identified artifacts which was revealed and pointing at the username associated within the used VM.

Finally, and the most important artifact in any digital forensic investigation is the timeline of artifacts which were indicating the first run sign in date and time, installation time of checked of OneDrive, Last update of the OneDrive folder and finally, the last sing in time into OneDrive account. All pointed timeline artifacts which were mentioned in section 5.5 Table:6 is revealing the discovered findings of artifacts which can build up an important timeline of artifacts where it can lead to important event as well as events when analyzing digital devices. It is important to

note that values identified within registry in which is related to the timeline are displayed in decimals and hexadecimal. Therefore, it is important for examiners to convert those collected values to human readable formats.

B. Comparison with Existing Work

In term of related work of this study, there are several studies which has proposed techniques for discovering digital evidence from digital devices for different cloud storage applications such as Dropbox, GoogleDrive and iCloud. For instance, a study conducted by [15] indicates that the acquisition and finding of results of Dropbox application in the Android as well as iOS operating systems. It was determined the malicious activities which were conducted by attackers and the types of artifacts discovered was analyzed.

Moreover, [17] has conducted a client-side forensic analysis on Windows 10 Operating systems to discover all possible artifacts which can be left over from the Dropbox application which was stored on Windows 10 OS. Artifacts of Windows registry were also included whereas the study has searched different investigations setup for the forensic analysis to adopt a conceptual digital forensic framework in the investigation process. This study has increased the learning of cloud storage forensics and the significance of registry investigation during digital investigations.

However, most of these studies only focuses on different type of OS and different type of cloud storage application. Therefore, the proposed analysis process involves applying different use cases and scenarios to ensure most of the registry artifacts has been covered and collected. Therefore, this study is unique as the Windows 11 Operating System introduced at the last quarter of 2021and registry result of identified artifacts will possibly be different on such as upgraded Operating System.

C. Limitations of The Research

The limitations of this study could be the actual digital forensic analysis of the actual OneDrive platform. However, this is impossible due to the privacy, terms, and conditions of OneDrive. Also, requesting actual access to the platform for studies purposes will require time to grant the required approval. Additionally, one of the limitations is that the implemented bash script will only work in Windows environment and will not work in Linux OS due to the different architecture between the two OS. Finally, there is a limitation of resources. For example, there is no open-source tools in which can perform cloud forensics and apply required techniques. Also, there is no tools identified to collect the total number of Windows registry keys and values. This would help to build a graphical view of the Windows registry during the development of this research as well as make it easier to track registry changes based on the changes of number of keys and values.

7. CONCLUSION

This research studies Windows 11 artifacts in the era of digital forensics of cloud storage applications. The use of cloud storage drives has become more popular, especially for students and business to share all resources among all authorized parties at the same time it created high availability of resources. However, attackers start using those cloud storage applications in way that data breaches could occur without the need of having physical storage devices such as USB or HDD drives. This research showed the different types of available cloud modules as well as available cloud services and discussed the main differences between them. This research also conducted a practical simulation to discover all identified artifacts which is related to OneDrive application. Moreover, with the help of Windows 11 virtual machine, simulations have been done in two different scenarios to track changes of the registry in both scenarios and collect all possible artifacts.

Furthermore, this research has discovered different artifacts when OneDrive application was linked to an account as well as when OneDrive was unlinked and uninstalled from the virtual machine. All findings from all simulations were incredible and can help a digital forensic investigator to determine if an attacker used OneDrive application to breach data. Also, the findings and left over artifacts help to identify the email account that was associated within OneDrive as well as file path for all uploaded files within OneDrive. It is important to note that timeline artifacts were also discovered during the practical experiments. For instance, the first time and date that OneDrive was running and signed into, the installation time of OneDrive was also discovered as well as the last sign in time.

Finally, a bash script was created and attached into the appendix to collect the identified and discovered artifacts which were gathered in the practical simulations to help digital forensic investigator to quickly determine if there is a use of cloud storage application or not. Also, it could be used as a lead to get known the attackers by known the accounts and the timeline that was OneDrive in use.

A. Future Work

In term of the future work which can be done to possibly improve the world of digital forensics in the era of cloud computing is to include additional cloud storage drives such as Dropbox and Google-Drive to discover any left behinds artifacts on Windows 11 registry. One the other hand, and as the use of Linux Operating System become more popular due to its advanced security similar simulation and analysis could possibly be done on Linux OS and compare all gathered artifacts and compare the differences in both Operation Systems.

References

[1] S. Ortiz Jr, "The problem with cloud-computing standardization," *Computer*, vol. 44, no. 07, pp. 13–16, 2011.

[2] N. Clarke, T. Tryfonas, and R. Dodge, *Proceedings of the Sixth International Workshop on Digital Forensics and Incident Analysis*. Plymouth: University of Plymouth, 2011.

[3] T. Fisher, "What Exactly Is a Registry Key?" https://www.lifewire.com/what-is-a-registry-key-2625999, 17 May 2022.

[4] H. K. Bella and S. Vasundra, "A study of security threats and attacks in cloud computing," in *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, 2022, pp. 658–666.

[5] P. R. Brandao, "Forensics and digital criminal investigation challenges in cloud computing and virtualization," *American Journal of Networks and Communications*, vol. 8, no. 1, pp. 23–31, 2019.

[6] S. Smith, "Cyber Security Breaches Report of Black Hat Ethical Hacking," https://www.blackhatethicalhacking.com/, 2019.

[7] V. Website, "Data Breach Investigations Report," https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf, 2020.

[8] N. K. Sehgal, P. C. P. Bhatt, and J. M. Acken, "Additional security considerations for cloud," in *Cloud Computing with Security*. Springer, 2019, pp. 193–215.

[9] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *IEEE Access*, vol. 8, pp. 131 723–131 740, 2020.

[10] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of internet services and applications*, vol. 4, pp. 1–13, 2013.

[11] B. T. Rao *et al.*, "A study on data storage security issues in cloud computing," *Procedia Computer Science*, vol. 92, pp. 128–135, 2016.

[12] Y. Zhang, C. Xu, and X. S. Shen, *Data security in cloud storage*. Springer, 2020.

[13] A. A. Adesina, A. A. Adebiyi, and C. K. Ayo, "Identification of forensic artifacts from the registry of windows 10 device in relation to idrive cloud storage usage," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 521–529, 2022.

[14] P. Prajapati and P. Shah, "A review on secure data deduplication: Cloud storage security issue," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 396–407, 2022.

[15] O. L. Carroll, S. K. Brannon, and T. Song, "Computer forensics: Digital forensic analysis methodology," 2017.

[16] S. Thorpe, "An experimental survey towards engaging trustable hypervisor log evidence within a cloud forensic environment," *International Journal of Computer Science & Information Technology*, vol. 4, no. 6, pp. 125–141, 2012.

[17] P. D. S. Lim, A. Johan and N. Ismai, "Dropbox forensics: Forensic analysis of a cloud storage service," *International Journal of Engineering Trends and Technology*, vol. 34, no. 7, pp. 2–9, 2020.

Mohammed A. Bajahzar A postgraduate student at Majmaah University, studying MSc in Cybersecurity and Digital Forensic. Full Time employee in one of the Saudi Arabian governmental sector. Current title is Incident Response and Digital Forensic Manager.

Prof. Shailendra Mishra Professor in the Department of Information Technology, College of Computer Information Science at Majmaah University. A professional with 20+ years of teaching experience and 28+ years of research experience.