International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Jul-24)

https://dx.doi.org/10.12785/ijcds/160102

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

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

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

Received 21 Apr. 2023, Revised 24 Feb. 2024, Accepted 6 Apr. 2024, Published 1 Jul. 2024

Abstract: Cloud storage drives have become very popular around the world these days. In the traditional approach to computer forensics, the focus is on physically accessing the disks that contain the information that could contribute to the factors. Due to the data breaches that can occur through cloud-based applications, the research proposed in this paper focuses on collecting evidence from Windows 11 operating systems to discover and collect leftover registry artefacts from one of the major cloud storage applications, OneDrive. This research study examined Windows 11 artefacts and found distinct artefacts when the OneDrive program was deleted from the virtual machine and unlinked to an account. The results and lingering artefacts assist in determining the file path for each uploaded file in OneDrive as well as the email address that was linked to it. To assist digital forensic investigators in making an expedient determination regarding the use of cloud storage applications, a bash script was developed and appended to the document. Its purpose is to assemble the identified and discovered artefacts that were obtained throughout the practical simulations. Identifying the accounts and the chronology that were using OneDrive, may also be utilized as a lead to identify the attackers.

Keywords: Digital Evidence, Cloud Forensic, Windows 11 Registry, Forensic artefacts, Cybersecurity.

I. Introduction

As technology evolves, new cloud storage applications are being introduced, bringing new challenges for digital forensics and law enforcement [1]. A cloud storage system may be created and built to store just certain kinds of data, such as digital images, picture files, or audio files. Concerns about security and privacy, shared technology, and outages that could compromise the dependability and availability of cloud storage services are a few particular problems with cloud storage [2],[3]. Cybercrime: cyberattacks such as ransomware, phishing, and denial-of- service attacks may target cloud storage providers or consumers [3], [4]. Government intrusion, server location, performance, latency, and compliance may all be impacted [5]. This research aims to examine and identify the registry artefacts collected and retrieved during a forensic cloud investigation and evaluate the applicability and effectiveness of the methods used to obtain the data in the Windows 11 registry. The purpose of this research is to set up a scientific experiment that demonstrates and compares what changes cloud storage applications can make to the Windows 11 registry. The experiment was configured so that it can be performed step by step and the same results will be obtained. This study produces a summary of Windows registry artefacts caused by cloud applications during installation and removal. Modern cloud storage applications allow organizations and users to transfer, upload, and store their data in the digital world. The increasing popularity of cloud storage applications among individuals and users could increase the possibility of data integrity loss, which increases users' concern about the security and protection of their important files and documents stored remotely [6]. The method used in this proposed research is to identify, retrieve, and analyze data from the Windows 11 registry that can be presented as credible evidence in a court case, which is referred to as digital forensics. This discipline uses various approaches, techniques, and technologies to achieve its goals. The data extraction process may be different for each device or kind of data to be examined, depending on the specifics of each situation [7].

Capturing and analyzing data from a traditional computer memory requires a different method than capturing and analyzing data over a live network and is another process for cloud-based technologies that involve partitioning of evidence and distributed settings Regardless of how the investigation is conducted, some forensic processes must be done extremely carefully to collect and store reliable digital information [8].

There are no specialized techniques in cloud forensics

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

and there is a lack of knowledge and professionals who know how to use them [3]. This problem becomes even more difficult when the data is encrypted and loss of data control is a factor. Building a forensic cloud capability is a prerequisite for cloud companies and participants. Otherwise, they are vulnerable to ongoing issues such as criminal breaches and serious policy violations when conducting a cloud forensic investigation [9]. This is because they are more likely to face these challenges if there are no forensic capabilities in the cloud. Due to insufficient forensic expertise and preparation, investigators also face challenges in cooperating with law enforcement in situations involving the seizure of resources.

All previous studies and academic research that were done on the forensic artefacts of cloud storage applications have been done on Windows 10 Operating systems as well as on Mac OS [10], [11]. This study is unique to the Windows 11 Operating System. In addition, the result of identified artefacts will possibly be different such as an upgraded Operating System.

This research focuses on comparing the results between collected data from cloud applications in two main approaches. First, a snapshot of the registry is taken without unlinking the OneDrive application, and the collected evidence is analyzed to compare with the second approach, while the cloud storage application is unlinked and removed from the computer to compare the collected evidence with the first result.

The main objectives of this study are:

- To investigate the literature on registration artefacts related to cloud storage applications.
- Understanding the process and methodology used to obtain artefacts from cloud storage applications.
- Discover cloud storage artefacts and perform a forensic analysis to uncover these artefacts.
- Conduct a digital forensic experiment to discover Windows 11 registry artefacts.
- Identify all possible ways to retrieve digital evidence related to cloud computing to minimize incident response time.

Following is the rest of the article. In the second section, we discuss the state-of-the-art research carried out by various researchers recently. The methodology and framework proposed in Section 3 are described. The results of the experiments and discussions are discussed in Section 4. The conclusion of the work is summarized in section 5.

II. literature Reviews

In the related work section, the body of literature pertinent to the topic is evaluated, with an emphasis on cloud computing technology and 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. This will cover the principles that govern the cloud, the many cloud models, the services they provide, vitalized, multi-tenancy, cloud security issues, and so on. In [12],[13] authors discussed, issues relating to governance, management, jurisdiction rights, confidentiality, and legal considerations and the procedure for collecting digital evidence in the case in a cloud environment.

A. Security Issues Within Cloud Computing

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 has also stated that in 2019, 48% of firms recognize at least a single attack every month, and 62% of organizations are capable of reacting rapidly to a data breach [14].

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. Also, only 31% of businesses have faced a cyber-attack on their 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 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%.

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, and 72% of security breaches featured victims from major businesses. However, 58% of victims had their data exposed. On the other hand, it is important to mention that there are more commonalities including 86% of data breaches being economically motivated, 43% using online applications, 37% stealing credentials such as usernames and passwords, 27% ransomware malware attacks, and finally, 22% of data breaches are attempted by phishing emails [15].

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. If cloud providers cannot keep the minimum speed to develop their technology to identify and defend against cyberattacks, denial of service assaults may probably occur. Authors in [16] have covered several data encryption techniques, in the context of cloud storage, searchable encryption, attribute-based encryption, homomorphic encryption, and identity-based encryption. The integrity of the user's data is of the utmost importance, especially when cloud service providers modify user information [16]. Authors in [17] have covered several data encryption techniques, in the context of cloud storage, searchable encryption, attribute- based encryption, homomorphic encryption, and identity- based encryption

Vulnerability is a flaw in a system that makes it possible for an attack to be successful. Presented threats in the cloud computing field include data scavenging where device or memory destruction is required, account or service hijacking, DDoS attacks, leakage of data, third- 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 to obtain sensitive information.

Problems with cloud storage include data integrity, data privacy as well as data recoverability, and data backup are discussed in [2], [5] Cloud computing also faces challenges in terms of adequate media refinement. There are still unresolved research difficulties in the area of cloud security that need to be further examined and analyzed when data comes to the use of encrypted deduplication in conjunction with symmetric key searchable encryption [18].

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. 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 [19].

Furthermore, Users can adjust cloud data storage to fit their requirements since it provides access to a large pool of shared resources. Some cloud service providers such as OneDrive, Azure, Google Drive, Alibaba, and IBM Cloud are well-known cloud storage applications that offer a variety of security options to protect user's data as well as user privacy [20]. OneDrive may be given high priority [21]. After OneDrive, the use of Google Drive 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.

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 realize what the term ”computer forensics” refers to or the processes that are engaged. There is a lack of comprehension of the distinction that may be made between the data extraction and the data analysis procedure. The following are key components of computer forensic examinations [22], [23]:

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

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. 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.

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 procedure that is included in the methodology. 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 need to be investigated.

D. *Research Gap*

The research gap in previous findings are:

- The types of registry artefacts that could be collected from Windows 11 OS when performing cloud-based forensic investigation.
- The relationship between registry artefacts and cloud applications in terms of their metadata such as installation data and linking, unlinking, and uninstallation date.

- Methods to discover forensic artefacts of cloud storage applications and how possible to discover all related forensics artefacts.

- Identify all possible ways of retrieving digital evidence related to cloud computing which will minimize the incident response timeline.

E. *Research Challenges*

Research Challenges are:

- Lack of time for expected delivery.

- Expensive software license for cloud forensics.

- The required intensive knowledge of digital forensic analysis skills.

- Lack of academic resources related to digital forensics for cloud infrastructures.

Research Questions are:

- What registry artefacts can be found when cloud applications are installed or uninstalled?

- What is the process and methodology of obtaining artefacts of cloud storage applications when installed on the Windows 11 Operating System?

- How do discover forensic artefacts of cloud storage applications and how to perform forensic analysis to discover those artefacts?

- How to identify all possible ways of retrieving digital evidence related to cloud computing that will minimize incident response timeline?

III. Research Methodology

The methodology of this research involves a practical simulation of registry artefacts collections whereas a study of all possible changes in the registry will be monitored and tracked during the installation and removal of the OneDrive cloud application. A bash script was implemented to improve the collection of registry values and artefacts which is related to cloud storage application. The objectives mentioned in the previous section would be fulfilled by using the following research methodology which is shown in Figure 1 below:

The above figure 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 be taken to gather artefacts and possible retrieval artefacts.

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

A. *Research Questions*

- When performing a digital forensic investigation on a Windows 11 registry based on cloud storage applications, what type of artefacts can be collected and gathered?

- How are registry artefacts related to cloud applications when installed?

- What is the process and methodology of cloud storage applications when installed on the Windows 11 Operating System?

- How to discover forensic artefacts of cloud storage applications and how to perform forensic analysis to discover those artefacts?

- How to identify all possible ways of retrieving digital evidence related to cloud computing which will minimize incident response timeline?

B. *Asserted Main Hypothesis*

Forensic artefacts can be found and seen when analysing the Windows registry.

- Hypothesis 1: The snapshots taken before and after the installation of the applications should illustrate different results.

- Hypothesis 2: There will be forensic artefacts left behind after the unlinking of the cloud storage applications.

C. *Proposed Scenario for System Modelling*

Figure 2, shows the proposed scenario whereas the suggested system Modelling can be used as a solution that will collect all gathered registry artefacts of the OneDrive application. It is important to explain each step within the proposed system to ensure how it works and to measure its effectiveness in the below steps:

1) The 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.

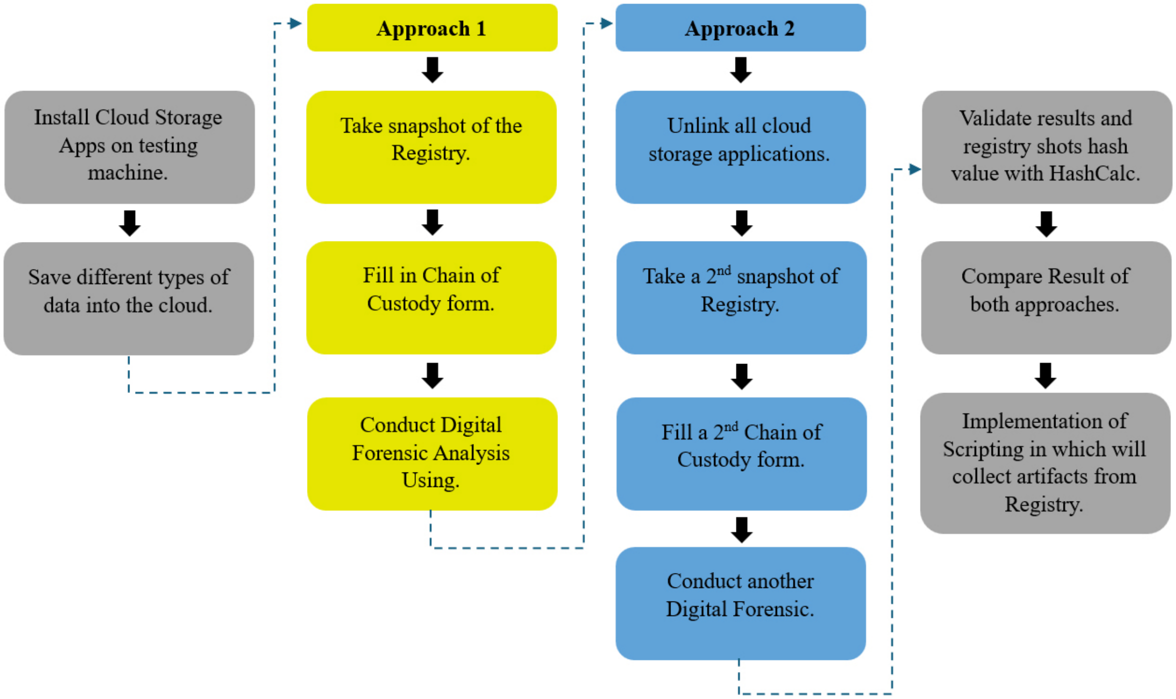

Approach 1
Approach 2
Install Cloud Storage Apps on testing machine.
Save different types of data into the cloud.
Take snapshot of the Registry.
Fill in Chain of Custody form.
Conduct Digital Forensic Analysis Using.
Unlink all cloud storage applications.
Take a 2nd snapshot of Registry.
Fill a 2nd Chain of Custody form.
Conduct another Digital Forensic.
Validate results and registry shots hash value with HashCalc.
Compare Result of both approaches.
Implementation of Scripting in which will collect artifacts from Registry.

Figure 1. Research Methodology and used approach.

4) The attacker has determined the routing table and knows the host VLAN.

5) The internal firewall was successfully passed.

6) Windows 11 system has been compromised and the attacker’s OneDrive account has been linked to the compromised machine to leak organization data.

7) The attacker started to upload data into the OneDrive storage.

8) With the help of the Digital Forensic Lab and implemented scripts, registry artefacts have been collected to take advantage of leftover artefacts or leads to know the identity of the attacker.

D. *System Modeling Architecture*

The proposed system modelling architecture will help to collect all related artefacts that will be discovered during the practical experimental shown in Figure 3. The below figure indicates how exactly will the system work from the start of establishing a connection from the digital forensic machine till the result gathering for analysis:

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

2) The suggested bash script will be copied into the infected machine to be run as an administrator.

3) The script will use a Windows CMD terminal to run the bash script as Windows admin.

4) The CMD terminal will request queries from the Windows registry of the infected machine to collect all required artefacts that are related to the OneDrive application.

5) All observed artefacts will be saved into a text file containing the identified keys and values of the Windows registry.

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

IV. Experimental Setup

The experiments were conducted using VMware Workstation V16.0.0. Windows 11 (64-bit) will freshly be installed with the following configurations:

(A) 30 GB of hard disk.

(B) 4 GB of memory.

(C) Guest OS will be allocated with 8 processors.

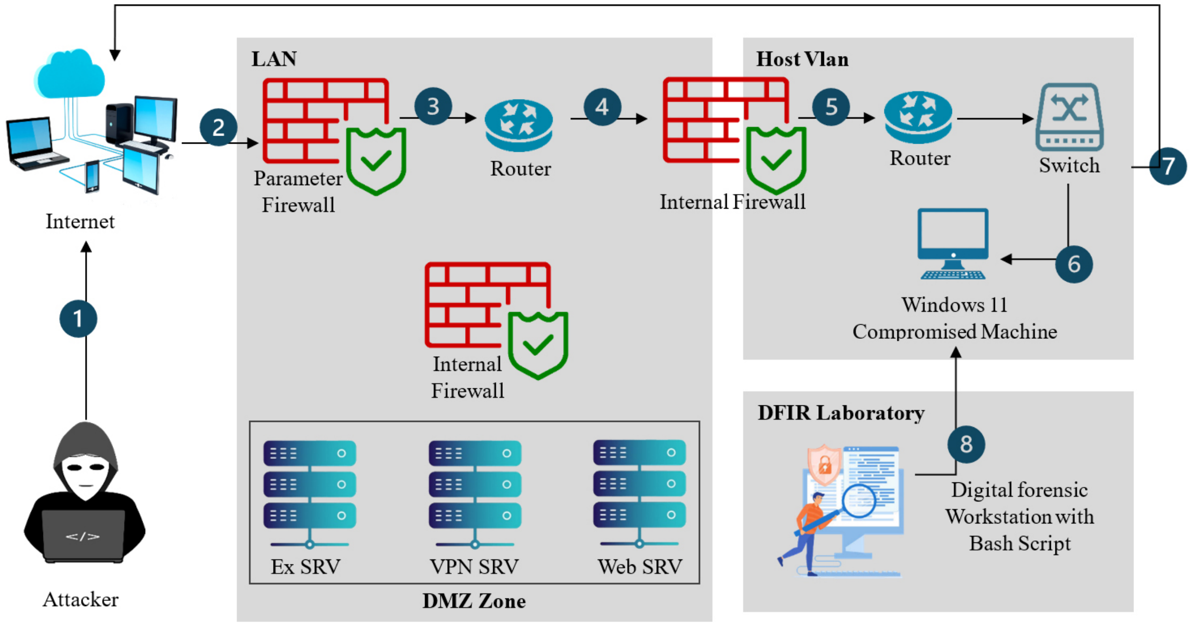


Figure 2. Proposed Scenario for System Modeling Usage

(D) The time zone was adjusted to +3GMT (Saudi Arabia) after the first boot-up, and the 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 the Regshot application (v1.9.7) and 7Zip (v24.5) to keep track of the changes in the Windows 11 registry.

(F) A total of two snapshots will be taken before and after the linking and unlinking of the OneDrive Application.

The experiments were based on OneDrive artefacts produced by the Windows registry. However, the focus of this practical simulation is primarily on the monitoring of the changes that occurred on the Windows registry. OneDrive was linked to an official Majmaah University account, files were uploaded, the account was unlinked, and the OneDrive application was uninstalled from Windows 11 to analyze leftover artefacts. The way that the OneDrive application interacts and behaves 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 them in terms of the following instances:

(A) After Linking OneDrive to an account and uploading 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 artefacts on the registry.
4) Keywords search via snapshot result.

The process graph (Figure 4) shows the life cycle which was followed to complete the experiment.

V. Results and Discussion

Linking, unlinking, and removing the OneDrive application on the virtual system resulted in the discovery of Windows registry artefacts. 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 artefacts. This section provides a list of findings, along with their values from a forensics perspective, and further extensive analysis of all identified forensics artefacts in the subsections below.

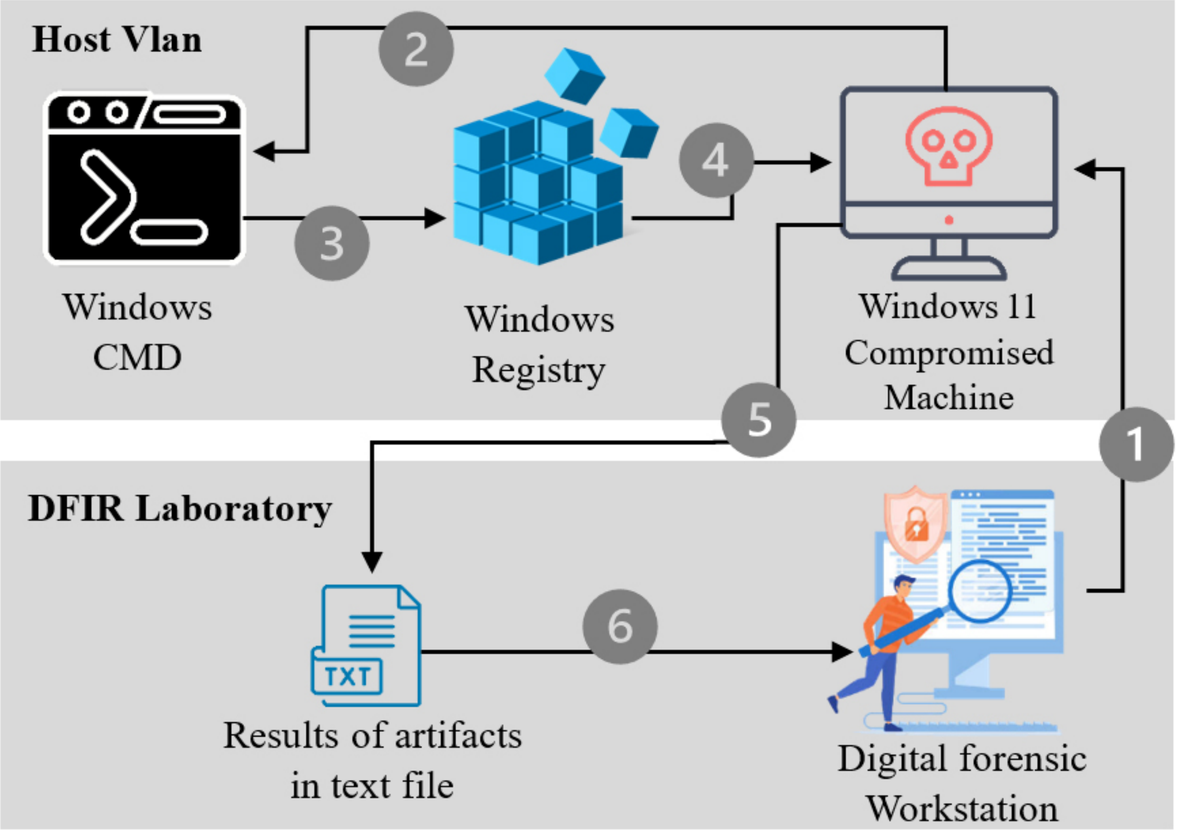

Host Vlan
Windows CMD
Windows Registry
Windows 11 Compromised Machine
DFIR Laboratory
TXT
Results of artifacts in text file
Digital forensic Workstation
1
2
3
4
5
6

Figure 3. Data Load

A. *Discovered Artefacts after Unlinking & Removing OneDrive*

The implemented script functionality shown in Table I, was conducted because of this experiment whereas registry key, values, and artefacts can be manually collected via the Command Prompt and all identified results will be saved on a txt file named RegistryCollecterResults.txt

It is important to note that after unlinking and uninstalling the OneDrive storage application from the targeted VM, some of the artefacts were left behind and can be used as a trace of evidence during any digital forensic investigation. All identified and discovered artefacts are shown in Table II. OneDrive network states that cache SSO was one of the artefacts that 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 with a OneDrive account.

Drive App ID is a discovered artifact that 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 the OneDrive app has been launched. Also, after uninstalling OneDrive, a deleted directory was created under the account directory which also indicates a deletion of the OneDrive Application.

B. *Configuration Settings Artefacts*

As part of the analysis, the configuration settings artefacts have been revealed which is helpful for the investigator to determine the locations of the OneDrive storage application.

- Silent business configuration was completed; this indicates the OneDrive application has been connected to a business account. This can be discovered from below registry path below:

  ```
  HKEY_CURRENT_USER\Software\Microsoft\
  OneDrive\SilentBusinessConfigCompleted
  ```

- The installation path for the OneDrive application was on the following path:

  ```
  Users\431104384\AppData\Local\Microsoft\
  ```

TABLE I. Implemented Script Functionalitys

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 the registry 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 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 the registry which is related to OneDrive.
`& RegQuery "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1"/v"UserEmail"> C:\Users\431104384\Desktop\RegistryCollectorResults.txt`	Request for User Email Address from the registry which is related to OneDrive.
`& RegQuery "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1"/v"UserFolder"> C:\Users\431104384\Desktop\RegistryCollectorResults.txt`	Request for User folder from the registry 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 the registry.
`&RegQuery"HKEY_CURRENT_USER\Software\Microsoft\OneDrive\23.048.0305.0002"/v"InstallPaths"> C:\Users\431104384\Desktop\RegistryCollectorResults.txt`	Request for OneDrive installation path from the registry.
`& RegQuery "HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1"/v"DisplayName"> C:\Users\431104384\Desktop\RegistryCollectorResults.txt`	Request for OneDrive Display name from the registry.
`& RegQuery "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.
`& RegQuery "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 the registry.
`& RegQuery "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 the registry.
`& RegQuery "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.

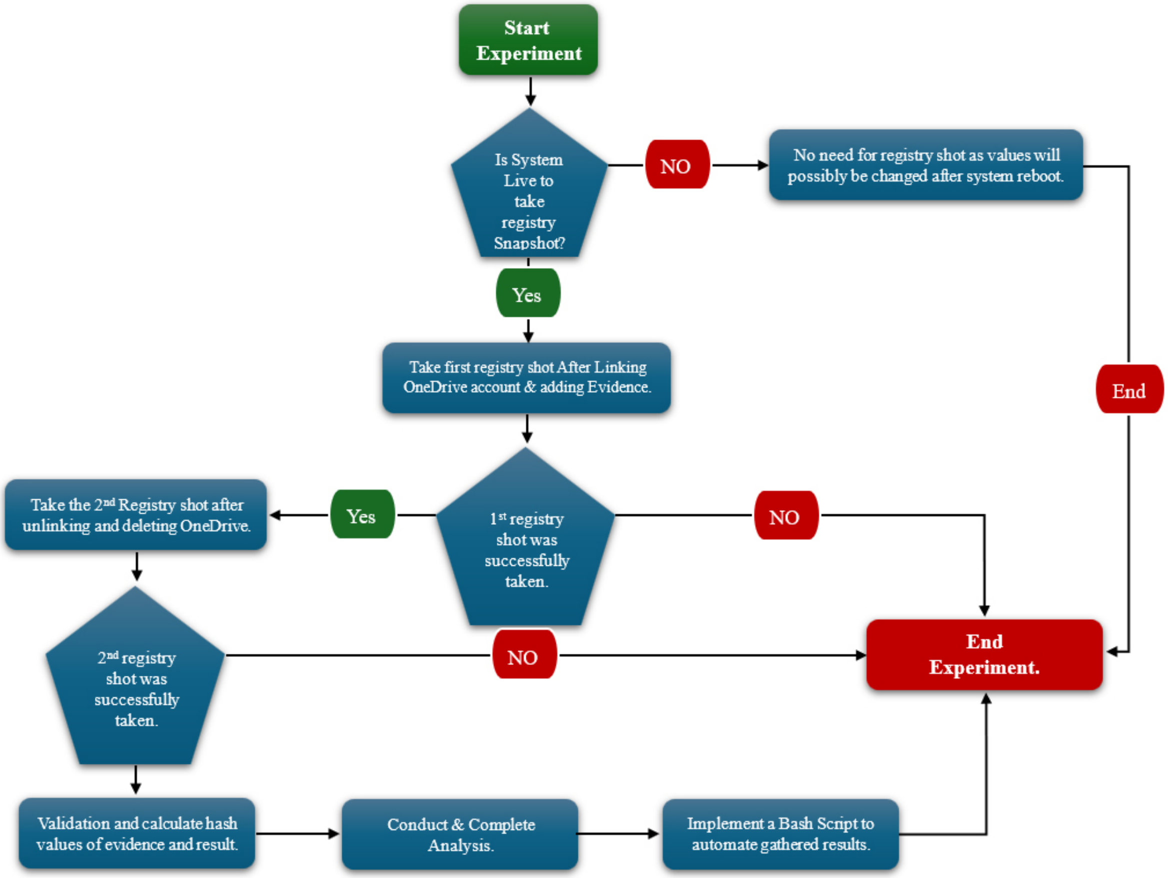

Start Experiment
Is System Live to take registry Snapshot?
NO
No need for registry shot as values will possibly be changed after system reboot.
Yes
Take first registry shot After Linking OneDrive account & adding Evidence.
End
Take the 2nd Registry shot after unlinking and deleting OneDrive.
Yes
1st registry shot was successfully taken.
NO
2nd registry shot was successfully taken.
NO
End Experiment.
Validation and calculate hash values of evidence and result.
Conduct & Complete Analysis.
Implement a Bash Script to automate gathered results.

Figure 4. Experiment Life Cycle

TABLE II. Discovered Artefacts after Removing OneDrive

Sub-Keys	Key Locations
OneDrive Network states that 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\23.043.0226.0001
HKEY_CURRENT_USER\Software\Microsoft\
OneDrive\23.043.0226.0001\InstallPath
```

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

```
HKEY_CURRENT_USER\Software\Microsoft\
OneDrive\Version
```

- Once unlinking OneDrive account has been initiated, OneDrive Icon has been changed from available and colourful icon to grey unavailable icon . This indicate OneDrive account has been signed off and it is needed to sign on again to sync.

```
HKEY_CURRENT_USER\Software\Microsoft\
OneDrive\HasSystrayIconBeenPromoted
```

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

```
HKEY_CUR0RENT_USER\Software\Microsoft\
OneDrive\UserInitiatedUninstall
```

C. Associated User Account-Related Artefacts

- 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 below:

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

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

```
HKEY_CURRENT_USER\Software\Microsoft\
OneDrive\UserDomainCollection0
```

- The hostname of the collection VM was discovered as ”Mohammed”. This is helpful as one of the identified artefacts was revealed and pointed at the username associated with the used VM. This can be discovered from below registry key below:

```
HKEY_CURRENT_USER\Software\Microsoft\
OneDrive\HostNameCollection
```

D. Timeline Related Artefacts

- OneDrive application is using the following user account which is related to the experimental Windows account: “431104384”. Its saved location can be found on the following:

```
C:\Users\431104384\AppData\Local\Microsoft\
OneDrive
```

E. Artefacts that reveal details of a directory

- The 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"
```

- 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 artefacts 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
```

- The business account was pointing at Majmaah SharePoint. This is helpful as it is indicating the associated account was a 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 below:

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

F. Result Comparisons

- Comparing between 1st & 2nd Registry Shot As discussed in the 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. Timeline Artefacts are shown in Table III and Table IV, which show the differences between both registries in terms of the keys and values.

- Script Results The below Figure 5 indicates the results that will be collected by the script that was explained in the Implemented Script. The script will

TABLE III. Timeline Artefacts

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

TABLE IV. Result in 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 ”container objects in which is similar to folders.” Keys in the registry may contain subkeys and values.	Key deleted suggests 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 2544 Values added 445 Values modified	In the registry, values hold certain instructions that applications in Windows will refer to [16].	Deleted values will most likely be the values that were associated with the deleted key above. 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.
326745 Total N.of Changes	All changes occurred between the 2 registry shots including the deleted keys and values as well as added and modified values.	

help investigators in their analysis during a data breach investigation and will save their time and effort once a registry investigation is required, instead of checking each registry hive, keys, and values one by one, the script will collect all relevant artefacts to OneDrive application and represent it in a .txt file as an output.

G. Discussions

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

Initially, for Linking account artefacts, there was a file launch registry value observed which indicates there is a use of OneDrive Application. In addition, OneDrive updates were triggered and detected via the registry which means that the OneDrive application was looking for the last updated version since it was linked to a user.

Secondly, after unlinking and uninstalling OneDrive from the application list, some artefacts occurred on the 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, an uninstallation key of OneDrive was added as well and a OneDrive deleted directory was initiated in the registry.

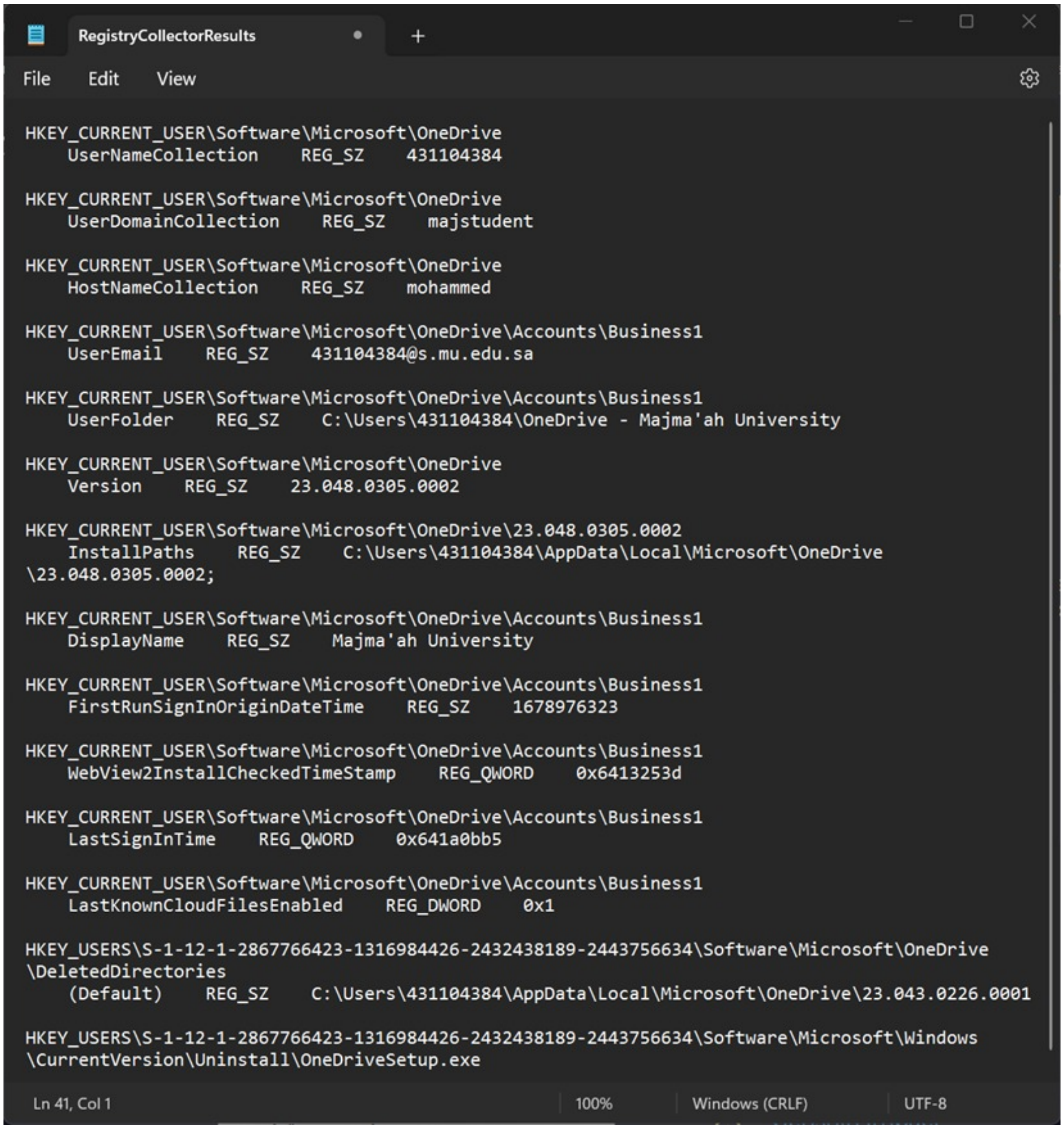
Thirdly, the configuration settings artefacts have been revealed which contain configuration artefacts for both approaches which can be helpful for the investigator to determine the path and folder of the location for the OneDrive storage application, and the post-authentication conditions have been discovered to have the value 1 which indicate there was a successful authentication for the business account on OneDrive as well as the installed version of OneDrive. Moreover, the last migration folder indicates the value of 1, this means it is true that the files uploaded from the cloud included: pictures, Screenshots, and Desktops. However, once unlinking the OneDrive account has been initiated, the OneDrive Icon has been changed from an available and colorful icon to a grey unavailable icon. This indicates the OneDrive account has been signed off and it is needed to sign on again to sync. For example, the Username Collection was pointing to 431104384@s.mu.edu.sa. Which is the account that was used to sign into OneDrive. Furthermore, the User domain collection associated with the login account to Windows is shown as ”Majstudent” Which is related to the Majmaah University domain associated with Microsoft services. Finally, the Hostname of the collection VM was discovered. This is helpful as one of the identified artefacts was revealed and pointed at the username associated with the used VM.

The most important artifact in any digital forensic investigation is the timeline of artefacts which indicates the first run sign-in date and time, installation time of checked OneDrive, Last update of the OneDrive folder, and finally, the last sign-in time into the OneDrive account. All pointed timeline artefacts that were mentioned in the Table reveal the discovered findings of artefacts which can build up an important timeline of artefacts where it can lead to important events as well as events when analyzing digital devices. It is important to note that values identified within the registry which are related to the timeline are displayed in decimals and hexadecimals. Therefore, examiners need to convert those collected values to human-readable formats.

In terms of related work of this study, several studies have proposed techniques for discovering digital evidence from digital devices for different cloud storage applications such as Dropbox, Google, and iCloud. For instance, a study conducted by [20] indicates the acquisition and finding of results of the Dropbox application in the Android as well as iOS operating systems. It was determined the malicious activities were conducted by attackers and the types of artefacts discovered were analyzed.

Moreover, [22] has conducted a client-side forensic analysis on Windows 10 Operating systems to discover all possible artefacts that can be left over from the Dropbox application which was stored on Windows 10 OS. Artefacts of the Windows registry were also included whereas the study has searched different investigation setups 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 focus on different types of OS and different types of cloud storage applications. Therefore, the proposed analysis process involves applying different use cases and scenarios to ensure most of the registry artefacts have been covered and collected.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 study purposes will require time to grant the required approval. Additionally, one of the limitations is that the



```
HKEY_CURRENT_USER\Software\Microsoft\OneDrive
    UserNameCollection    REG_SZ    431104384

HKEY_CURRENT_USER\Software\Microsoft\OneDrive
    UserDomainCollection    REG_SZ    majstudent

HKEY_CURRENT_USER\Software\Microsoft\OneDrive
    HostNameCollection    REG_SZ    mohammed

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    UserEmail    REG_SZ    431104384@s.mu.edu.sa

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    UserFolder    REG_SZ    C:\Users\431104384\OneDrive - Majma'ah University

HKEY_CURRENT_USER\Software\Microsoft\OneDrive
    Version    REG_SZ    23.048.0305.0002

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\23.048.0305.0002
    InstallPaths    REG_SZ    C:\Users\431104384\AppData\Local\Microsoft\OneDrive
\23.048.0305.0002;

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    DisplayName    REG_SZ    Majma'ah University

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    FirstRunSignInOriginDateTime    REG_SZ    1678976323

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    WebView2InstallCheckedTimeStamp    REG_QWORD    0x6413253d

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    LastSignInTime    REG_QWORD    0x641a0bb5

HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Business1
    LastKnownCloudFilesEnabled    REG_DWORD    0x1

HKEY_USERS\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Software\Microsoft\OneDrive
\DeletedDirectories
    (Default)    REG_SZ    C:\Users\431104384\AppData\Local\Microsoft\OneDrive\23.043.0226.0001

HKEY_USERS\S-1-12-1-2867766423-1316984426-2432438189-2443756634\Software\Microsoft\Windows
\CurrentVersion\Uninstall\OneDriveSetup.exe
```

Figure 5. Script Collected Results in a text file.

implemented bash script will only work in a Windows environment and will not work in Linux OS due to the different architecture between the two OS. Also, there are 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 in several keys and values.

VI. Conclusion

This research studies Windows 11 artefacts in the era of digital forensics of cloud storage applications. The use of cloud storage drives has become more popular, especially for students and businesses 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 a way that data breaches could occur without the need to have 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 artefacts that are related to the OneDrive application. Moreover, with the help of a Windows 11 virtual machine, simulations have been done in two different scenarios to track changes in the registry in both scenarios and collect all possible artefacts. Furthermore, this research has discovered different artefacts 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 determine if an attacker used the OneDrive application to breach data. Also, the findings and leftover artefacts help to identify the email account that was associated with OneDrive as well as the file path for all uploaded files within OneDrive. It is important to note that timeline artefacts 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 to the appendix to collect the identified and discovered artefacts which were gathered in the practical simulations to help digital forensic investigators quickly determine if there is a use of cloud storage application or not. Also, it could be used as a lead to get to know the attackers by knowing the accounts and the timeline that was OneDrive in use.

In terms of the future work that 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 behind artefacts on the Windows 11 registry. On the other hand, as the use of the Linux Operating System become more popular due to its advanced security similar simulation and analysis could be done on Linux OS and compare all gathered artefacts and compare the differences in both Operation Systems.

References

[1] A. A. Khan, A. A. Shaikh, A. A. Laghari, and M. M. Rind, "Cloud forensics and digital ledger investigation: a new era of forensics investigation," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 1, pp. 1–23, 2023.

[2] M. Ali, L. T. Jung, A. H. Sodhro, A. A. Laghari, S. B. Belhaouari, and Z. Gillani, "A confidentiality-based data classification-as-a-service (c2aas) for cloud security," *Alexandria Engineering Journal*, vol. 64, pp. 749–760, 2023.

[3] Z. A. Hussien, H. A. Abdulmalik, M. A. Hussain, V. O. Nyangaresi, J. Ma, Z. A. Abduljabbar, and I. Q. Abduljaleel, "Lightweight integrity preserving scheme for secure data exchange in cloud-based iot systems," *Applied Sciences*, vol. 13, no. 2, p. 691, 2023.

[4] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-sdn-based secure architecture for cloud computing in smart industrial iot," *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421, 2023.

[5] L. Pons, J. Feliu, J. Sahuquillo, M. E. Gómez, S. Petit, J. Pons, and C. Huang, "Cloud white: Detecting and estimating qos degradation of latency-critical workloads in the public cloud," *Future Generation Computer Systems*, vol. 138, pp. 13–25, 2023.

[6] S. Peng, W. Bao, H. Liu, X. Xiao, J. Shang, L. Han, S. Wang, X. Xie, and Y. Xu, "A peer-to-peer file storage and sharing system based on consortium blockchain," *Future Generation Computer Systems*, vol. 141, pp. 197–204, 2023.

[7] M. Al Jouhi and S. Al Hosani, "Windows forensics analysis," *Emirati Journal of Policing & Security Studies*, vol. 1, no. 1, pp. 4–11, 2022.

[8] K. Y. Chan, B. Abu-Salih, R. Qaddoura, A.-Z. Ala'M, V. Palade, D.-S. Pham, J. Del Ser, and K. Muhammad, "Deep neural networks in the cloud: Review, applications, challenges and research directions," *Neurocomputing*, p. 126327, 2023.

[9] F. Iqbal, A. Jaffri, Z. Khalid, A. MacDermott, Q. E. Ali, and P. C. Hung, "Forensic investigation of small-scale digital devices: a futuristic view," *Frontiers in Communications and Networks*, vol. 4, p. 1212743, 2023.

[10] H. Bowling, K. Seigfried-Spellar, U. Karabiyik, and M. Rogers, "We are meeting on microsoft teams: Forensic analysis in windows, android, and ios operating systems," *Journal of Forensic Sciences*, vol. 68, no. 2, pp. 434–460, 2023.

[11] J. Joun, S. Lee, and J. Park, "Discovering spoliation of evidence through identifying traces on deleted files in macos," *Forensic Science International: Digital Investigation*, vol. 44, p. 301502, 2023.

[12] J. Singh, J. Cobbe, D. L. Quoc, and Z. Tarkhani, "Enclaves in the clouds: Legal considerations and broader implications," *Communications of the ACM*, vol. 64, no. 5, pp. 42–51, 2021.

[13] 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.

[14] H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using artificial intelligence," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 2020, pp. 829–836.

[15] V. (2022) Verizon business. [Online]. Available: https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf

[16] N. K. Sehgal, P. C. P. Bhatt, and J. M. Acken, "Cloud computing with security," *Concepts and practices. Second edition. Switzerland: Springer*, 2020.

[17] 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.

[18] 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. 3996–4007, 2022.

[19] A. Kumar, B. B. Kumar, S. Kalita, R. Chaganti, and P. Nand, "Controlling and surveying of on-site and off-site systems using web monitoring," in *Advanced Practical Approaches to Web Mining Techniques and Application*. IGI Global, 2022, pp. 14–35.

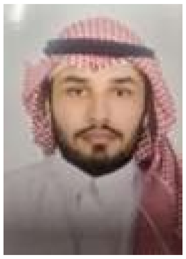
[20] S. Y. Lim, A. Johan, P. Daud, and N. Ismail, "Dropbox forensics: forensic analysis of a cloud storage service," *Int. J. Eng. Trends Technol*, pp. 45–49, 2020.

[21] P. Domingues, L. Andrade, and M. Frade, "A digital forensic view of windows 10 notifications," *Forensic Sciences*, vol. 2, no. 1, pp. 88–106, 2022.

[22] O. L. Carroll, S. K. Brannon, and T. Song, "Computer forensics: Digital forensic analysis methodology," *US Att'ys Bull.*, vol. 56, p. 1, 2008.

[23] A. A. Alhussan, A. Al-Dhaqm, W. M. Yafooz, A.-H. M. Emara, S. Bin Abd Razak, and D. S. Khafaga, “A unified forensic model applicable to the database forensics field,” *Electronics*, vol. 11, no. 9, p. 1347, 2022.

Shailendra Mishra , Shailendra Mishra (Senior Member, IEEE) received the Master of Engineering (M.E.) and Ph.D. degrees in computer science and engineering from the Motilal Nehru National Institute of Technology (MNNIT), India, in 2000 and 2007, respectively. He is currently working as Professor with the Department of Computer Engineering, College of Computer and Information Science, Majmaah University, Majmaah, Saudi Arabia. He has published and presented more than 90 research articles in international journals and international conferences. His current research interests include cloud and cyber security, SDN, the IoT security, communication systems, computer networks with performance evaluation, and design of multiple access protocol for mobile communication networks. He is a Senior Member of ACM, and a Life Member of the Institution of Engineers India (IEI), the Indian Society of Technical Education (ISTE), and ACEEE.



Mohammed A. Bajahzar , Master student in Cyber Security & Digital Forensics ,IT Deptt. Majmaah University, Saudi Arabia. His research interests include cloud security, cybersecurity, the IoT, semantic web, cloud and edge computing, and smart city and mathematical modeling of physical and biological problems in general and mathematical analysis.