Identification of forensic artifacts from the registry of windows 10 device in relation to idrive cloud storage usage

Adesoji A. Adesina[1], Ayodele Ariyo Adebiyi[2], Charles K. Ayo[3]
[1]Department of Computer and Information Science, Covenant University, Ota. Ogun State, Nigeria
[2]Department of Computer Science, Landmark University, Omu-Aran, Kwara State, Nigeria
[3]Department of Computer Science, Trinity University, Sabo. Lagos State, Nigeria

Article Info

Article history:

Received Jun 28, 2021
Revised Oct 10, 2021
Accepted Dec 21, 2021

Keywords:

Artifacts
Client-sides forensics
Cloud storage
Digital devices
Registry

ABSTRACT

The accessibility of cloud storage over the internet as a result of cloud computing technology provides the opportunity to store, share and upload data online with the use of digital devices which can be accessed anytime and anywhere. These benefits can also be exploited by the cybercriminals to perform various criminal activities including storing and exchanging of illegal materials on cloud storage platforms. The logs of malicious usages can be obtained from the cloud service providers for forensic investigations but the privacy issue among other factors make it difficult for such logs to be shared. Therefore, there is a need to perform client-side forensics to be able to carry out forensic investigation on digital devices as related to the activities on cloud storage. This study identifies relevant artifacts that can be forensically extracted from the registry of a window 10 device that accessed iDrive cloud storage. The study explores different experimental setups for the forensic analysis and adopted an integrated conceptual digital forensic framework in the investigation process to detect relevant forensic artifacts from the registry of a windows 10 device. This study increases the knowledge of cloud storage forensics and the significance of registry analysis during digital investigations.

Corresponding Author:

Adesoji A. Adesina
Department of Computer and Information Sciences
Covenant University, Ota Ogun State, Nigeria
Email: adesoji.adesina@stu.cu.edu.ng

1. INTRODUCTION

The innovation of cloud computing has revolutionized the way information technology (IT) services are being provisioned and deployed [1]. It is a service delivery model that enables its subscribers to access the cloud service using a thin client such as web browser through the internet at anytime (24/7), from anywhere and anyplace [2]. The service models in cloud computing as stated by national institute of standards and technology (NIST) includes: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) [3]. Storage as a service (STaaS) is an addition to these traditional service models [4] and is included in the IaaS model of cloud [5], [6].

The storage as a service (STaaS) allows cloud users to store their files online (that includes personal health records, emails, government sensitive files among others) and access the files anytime, anywhere, everywhere (24/7) through the internet digital devices as a result of their flexibility, affordability, and portability. Despite the benefits associated to the usage of cloud storage services, the security and privacy issues in the cloud domain are the major concerns to its subscribers, the forensics researchers, law enforcement agents and the practitioners [7], [8]. The increasing popularity of cloud storage platforms with their easy accessibilities on the Internet using digital devices such as mobile phones and computers couple with various malicious usages have made investigations into cyber domain difficult [9], [10].

Examples of cloud storage include google drive, media fire, onedrive, idrive icloud, dropbox, ubuntu one, pcloud and sugarsync among others. Different factors including the physical inaccessibility to the digital artifacts on the cloud servers that span across multiple jurisdictional areas, the integrity of the data artifacts that can be provided by the cloud service providers, the cloud architectures, the growing popularity of cloud storage platforms among others have increased and encouraged various forms of criminal activities these factors are also be identified to pose various challenges to the conduct of forensic investigation on cloud storage services [11].

As a result of the mentioned challenges, it is therefore essential to explore clients side forensics to identify, extract, analyze forensic footprints (artifacts) from digital devices malicious usages on cloud storage. Windows registry has been identified as one of the locations where forensic artifacts can be located to determine the various activities carried out on devices that are built on windows operating systems. It stores all hardware and software configurations, user activities and transactions [12], that allows it to provide relevant artifacts to assist in forensic investigation.

The purpose of this research is to identify the relevant artifacts from the registry of a windows 10 operating system device when an idrive cloud storage is used as a storage and deployment media and to show the behavior of cybercriminals in relation to the cloud storage usage. iDrive cloud storage offers online backup functionalities for all ranges of digital devices that run on windows, iOS and android operating systems but its features can also be exploited by the cybercriminals to carry out malicious activities. Forensic analysis on windows 10 devices that have accessed iDrive cloud storage is very limited in literature and needs to be further investigated to provide forensic guidelines for cybercrimes investigation on cloud storages.

2. RELATED WORK

Investigating cloud client devices are becoming a standard component of contemporary digital investigation cases as a result of various locations on the devices that provide useful evidential artifacts in relation to the cloud storage services usage [13], [14]. Many studies have been carried out on diverse strategies and techniques to perform forensic investigations on windows system, mac system, iphone and android smartphone to determine various usages on different cloud storage services [15]-[17].

The artifacts related to Google drive client was forensically extracted from windows 7 operating systems [18]. It was found that useful forensic artifacts can be located on Google drive after the usage of windows 7 and apple iPhone devices. Artifacts extracted include the username, the password, filenames of the documents accessed, dates and times the cloud storage was accessed. Blakeley *et al.* [19] investigated the different artifacts on microsoft windows 8.1 that can be found after the usage on hubic cloud storage. The authors presented different artifacts that were extracted when operations including upload, download, installation, and uninstallation were carried out. Satrya and Shin [20] analyzed and documented the different types of volatile and non-volatile data that were retrievable from windows 8, Mac OS X 10.9, android 4 and iOS 7 devices when a user carried out different activities such as upload and download of files and folders after the usage with sugarsync cloud storage. The authors were able to recover a number of useful artifacts with the traces of sugarsync after carrying out related activities on the cloud storage. Yang *et al.* [21] extracted the data remnants from the use of cooperative cloud storage services using symform as a case study. The authors investigated the terrestrial artifacts on the mobile devices and personal computers running various popular operating systems such as windows 8.1, Mac OS X mavericks 10.9.5, ubuntu 14.04 LTS, iOS 7.1.2, and android kitkat 4.4. Their research focus was to determine if the file contents and timestamps of the uploaded and downloaded files to and from the cloud storage were altered after the operations. The potential artifacts recovered during the research included data relating to the installation and un-installation of the cloud applications, log-in to and log-off from symform account using the client application, file synchronization as well as their timestamp information. Three cloud storages namely SpiderOak, JustCloud and pCloud on windows 8.1 and IOS 8.1.1 devices were investigated to locate the footprints left on them after the usage [22]. The focus of the research was to determine the forensic artifacts that can be retrieved from the random access memory (RAM), hard drive (HDD) on windows 8.1 devices after the usage of the SpiderOak, JustCloud and pCloud with the web browsers (internet explorer (IE), firefox (Fx) and google chrome (GC) and the client windows application on each of the cloud storage being examined. Data artifacts that could be extracted from dropbox cloud storage with the use of smartphone (android lollipop and android nougat) was investigated [23]. The common activities carried out in this work included installing, signing up, uploading, downloading and sharing operations. The artifacts extracted included the username, password, the modified files used during the activity, time and date of the activity, list of files uploaded by the user with information. Aggarwal *et al*. [24] described the design and implementation of data extraction system from mobile devices. The authors described the complete targeted data extraction system (TDES) and presented the results of the experiments conducted with both iOS and android based systems. The author based their experimental design on data identification, data acquisition and data validation based on online metadata based filtering, On-device content based filtering and off-device (backup) based filtering. using this approach, the authors were able to extract the following artifacts from the mobile devices being investigated; the contacts and address book, short message service (SMS), multimedia messaging service (MMS), calendar, voice memos, notes, photographs, video/audio, maps and location info, voice mails stored files, the browsing history, emails, social networking data, messaging data (text, voice, video, pictures) from whatsapp, facebook and skype. Rochmadi and Heksaputra [25] investigated artifacts that can be detected from the random access memory (RAM), logical drive and google chrome database from windows 10 device that was used to access adrive cloud storage. the national institute of standards and technology (NIST) forensic framework (comprising the acquisition/collection, examination, analysis, and conclusion/reporting stages) was used during the investigation process, while the methodology used involved literature review, preparation and identification, simulation and scenario, forensic investigation and reporting. The RAM and Windows logical system analysis with the use of autopsy 4.11.0 tool revealed the installation path of the application.

3. RESEARCH METHOD

It is very essential to follow forensic guidelines that provide concise, reliable and verifiable forensic results during forensic investigation. The research methodology proposed in this study will assist forensic investigators to be able to detect and extract forensic artifacts from the registry of a device running on Windows 10 operating systems that are related to the malicious usages on iDrive cloud storages and also provide guidelines to assist forensic examiners in the real-life examination of other cloud client applications on other digital devices.

3.1. The proposed digital forensic framework for cloud client devices

This research adapted the integrated conceptual digital forensic framework investigation used by [26]. The framework is depicted in Figure 1 as a four stages processes while the descriptions of the stages are presented in Table 1. The process is divided into four stages.

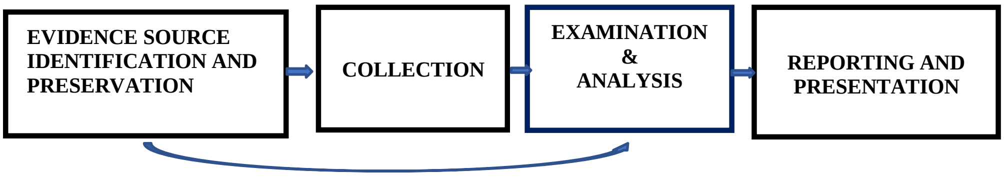

EVIDENCE SOURCE IDENTIFICATION AND PRESERVATION
COLLECTION
EXAMINATION & ANALYSIS
REPORTING AND PRESENTATION

Figure 1. An integrated conceptual digital forensic framework

Table 1. Description of the activities in the proposed framework

Stages	Description
Evidence source identification and preservation stage	This phase identifies the registry on a Windows 10 device as the main source where the digital artifacts can be located and extracted.
Collection	This phase is concerned with the actual capturing of the evidential data from the registry on the Windows 10 device identified in the previous phase. SysTracer utility tool was employed to locate the relevant artifacts from the registry keys.
Examination and analysis	This phase is concerned with the examination and analysis of the registry keys to examine and extract the identified traces of iDrive in the previous phase.
Reporting	This phase is concerned with the process of preparing and presenting the detailed reports of the findings.

3.2. The procedure for cloud storage client forensic in implementing the proposed framework

The activity workflow process that provided the necessary guidance in this research is depicted in Figure 2.

3.2.1. Experimental setup

The experimental setup was based on virtualization technique with setting up of different virtual machines to simulate different activities that can be performed on cloud storage. The procedures were carried out on a Dell laptop with windows 10 64 bit operating systems with the following specifications: 32GB RAM, Intel Core™ i-7-4810MQ, CPU@2.8GHZ and 1TB Hard drive. A virtual based machine named windows 10 Based VM will be created on the virtual host machine and will serve as the control system for this research using VMware players 15.5.014665864 with this configuration: windows 10 professional (64-bit operating system, with 2.80 GHz CPU, 2 GB of RAM and 35 GB of hard disks).

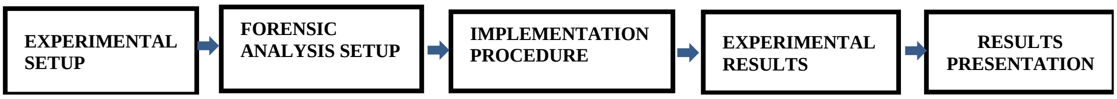


Figure 2. Activity workflow of the study

3.2.2. Forensic analysis setup

To perform Windows 10 application-based experiment in this study, six virtual machines were setup (VM1-VM6) as shown in Figure 3 representing the common activities that can be carried out on any cloud storage.

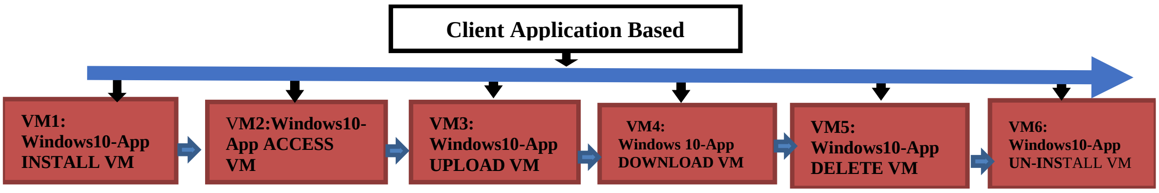

Client Application Based
VM1: Windows10-App INSTALL VM
VM2:Windows10-App ACCESS VM
VM3: Windows10-App UPLOAD VM
VM4: Windows 10-App DOWNLOAD VM
VM5: Windows10-App DELETE VM
VM6: Windows10-App UN-INSTALL VM

Figure 3. Activities on windows 10 application based VMs

3.2.3. Implementation procedures

The forensic analysis of registry to locate the relevant artifacts related to the usage of iDrive cloud storage on windows 10 device is presented in Figure 4.

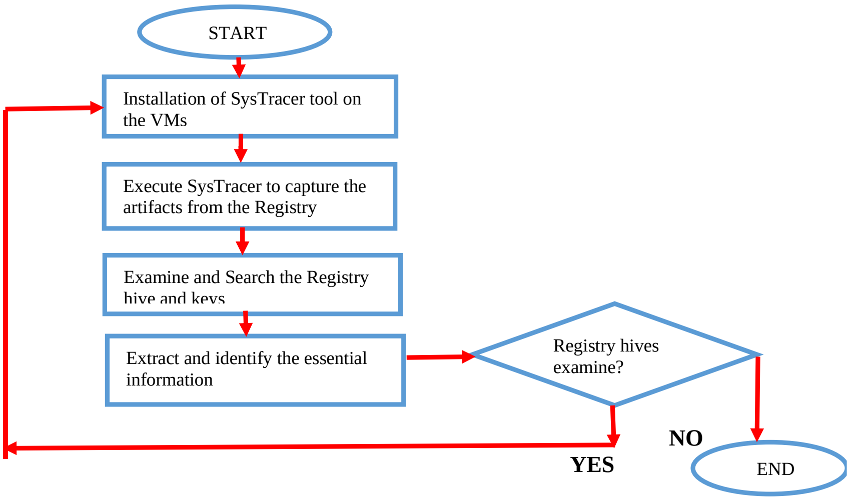

START
Installation of SysTracer tool on the VMs
Execute SysTracer to capture the artifacts from the Registry
Examine and Search the Registry hive and keys
Extract and identify the essential information
Registry hives examine?
NO
YES
END

Figure 4. The workflow process during the extraction of artifacts from the registry on windows 10 devices

The tool and the datasets used for the forensic analysis the registry of Windows 10 device to detect the traces of iDrive cloud storage is presented in Table 2.

Table 2. Forensic analysis of IDrive using registry keys analysis from windows 10 device

Task/activities performed	Description of the task	Version
Installation of SysTracer	Installation of SysTracer tool for the registry analysis	SysTracer version 2.10
Installation of the downloaded iDrive client app from the internet	Identification of relevant artifacts related to the installation and logon activities of iDrive usage	iDriveWinsetup.exe version 6.7.154
Upload, download and delete operations with the downloaded datasets	Datasets (pdf and mp4 files with terrorism contents) downloaded from the internet were used to determine the locations on the registry keys where the uploaded, downloaded, uninstallation and deletion activities can be detected	Nuclear-Security-Fact-Sheet.pdf, money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-an.pdf and Neutron Bombs Used In War of Yemen2015.MP4

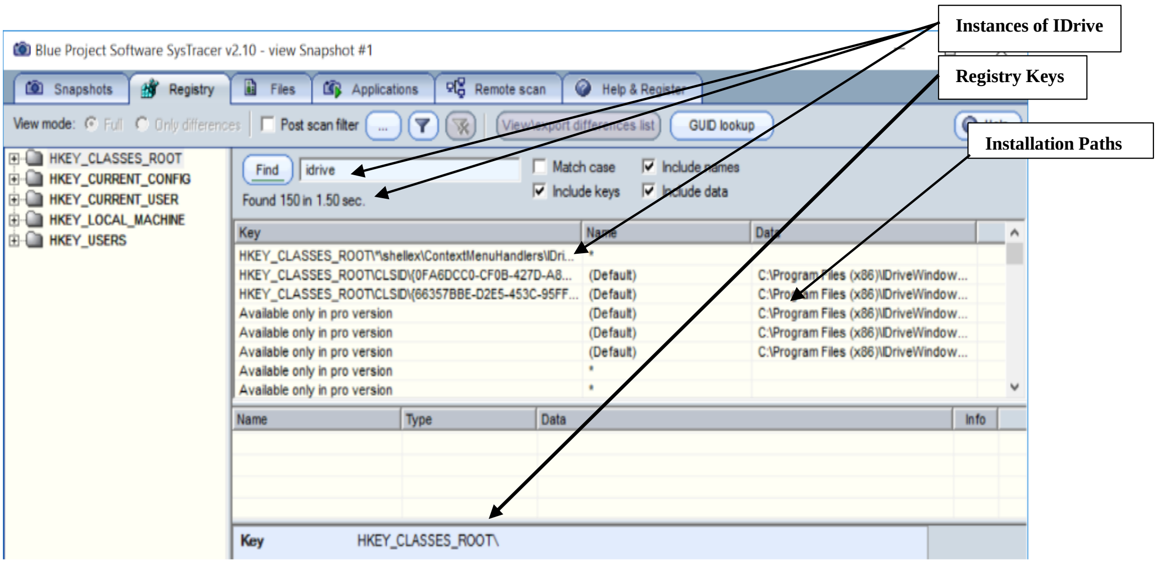
3.2.4. Experimental results

Table 3 presents the activities carried out on the different virtual machines (VM1-VM6) setup for the experiment, it presented the registry locations where relevant forensic artifacts related to the usage of iDrive can be obtained from Windows 10 device. As shown in Table 3, the experiment performed on VM1 showed that forensic artifacts related to the installation of iDrive Cloud Storage application can be obtained from the registry on Windows 10 device using appropriate forensic tool like SysTracer. The interface showed the extracted artifacts (Figure 5), the figure showed the different registry keys that contained the instances of the installation. The experiment on VM2 showed that the credentials (username) that user used to access the cloud storage can be identified from certain registry keys as presented in Figure 6. The experimental results on VM3, VM4, VM5 and VM6 showed the upload, download, delete and uninstall operations carried out on the respective virtual machines as related to the iDrive cloud storage usage with the extracted datasets as presented in Table 3 and illustrated in Figure 7 and Figure 8 respectively. Figure 7 revealed the uploaded dataset and the registry key that hold the data value. Figure 8 showed the downloaded dataset with the corresponding registry key.

Table 3. Experimental results

Virtual machine examined with the activities performed	Registry key searched	Result obtained
VM1: The downloaded iDrive app was installed on VM1. SysTracer was installed on VM1 to determine the relevant artifacts related to the installation.	HKEY_LOCAL_MACHINE\software\microsoft\windows\ currentversion\installer\folders HKEY_CURRENT_USER\SOFTWARE HKEY_USERS\S-1-5-18\SOFTWARE HKEY_CLASSES_ROOT\installer	Traces of iDrive client installed were identified on VM1 (Figure 5)
VM2: The installed iDrive client was accessed with a username (pstadesina@outlook.com) with a password. SysTracer was used to identify the username and password from the registry keys.	HKEY_CURRENT_USER HKEY_LOCAL_MACHINE\SOFTWARE\IDRIVEW HKEY_USERS\S-1-5-18\SOFTWARE\IDRIVEW	Username used to install the idrive client was identified on VMS identified. No traces of the password used was identified (Figure 6)
VM3: The datasets employed in this experiment (as presented in Table 2) are Nuclear-Security-Fact-Sheet.pdf, money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-an.pdf and Neutron Bombs Used In War of Yemen2015.MP4) were uploaded to the iDrive Cloud Storage to the possibility of identifying the datasets. The SysTracer tool was employed to identify or locate the registry keys where the uploaded documents and clips were located.	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\ Windows\CurrentVersion\ ExploreRecentDocs\. HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\ CurrentVersion\Explorer\RecentDocs\mp4	Uploaded documents and the video clip files were identified (Figure 7)
VM4: The uploaded documents and video clips (as presented in Table 2) were downloaded from the idrive into VM4. SysTracer tool was used to determine the registry keys where the downloaded documents and video clips were located.	CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\. HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf\ HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\mp4\	Downloaded documents and video clips identified (Figure 8)
VM5: The uploaded documents and video clips were deleted from the iDrive. SysTracer were used to locate the registry keys where the traces of the deleted items resided.	CURRENT_USER\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\RecentDocs\.	Deleted documents identified
VM6: The installed iDrive client was uninstalled from the control panel. SysTracer was used to determine the registry keys where the traces of the uninstallation operation were located.	HKLM\SOFTWARE\Microsoft\Windows\ Current\Version\Uninstall	Uninstalled program identified

The result of the registry keys analysis on the Windows 10 device when various cloud storage activities (including installation, login, upload, download, uninstallation, deletion operations) were carried out are presented in Table 3. The artifacts discovered from the different registry subkeys included the installation path of the iDrive, traces of the iDrive cloud storage installed, the account that was used to access the iDrive cloud storage, the documents and files(datasets) that were uploaded, downloaded, deleted, the traces of the uninstalled process. The experimental results show that valuable forensic artifacts of cloud drive activities can be identified from the registry of Windows operating system devices. The same relevant forensic artifacts can also be extracted when similar experimental activities are carried out on other cloud storages when used with other digital devices.



Blue Project Software SysTracer v2.10 - view Snapshot #1

View mode: ● Full ○ Only differences □ Post scan filter

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS

Find: idrive

□ Match case ☑ Include names
☑ Include keys ☑ Include data

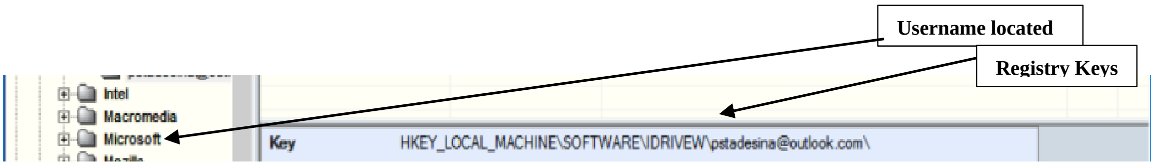
Found 150 in 1.50 sec.

Key	Name	Data
HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers\IDri...	*	
HKEY_CLASSES_ROOT\CLSID\{0FA6DCC0-CF0B-427D-A8...	(Default)	C:\Program Files (x86)\IDriveWindow...
HKEY_CLASSES_ROOT\CLSID\{66357BBE-D2E5-453C-95FF...	(Default)	C:\Program Files (x86)\IDriveWindow...
Available only in pro version	(Default)	C:\Program Files (x86)\IDriveWindow...
Available only in pro version	(Default)	C:\Program Files (x86)\IDriveWindow...
Available only in pro version	(Default)	C:\Program Files (x86)\IDriveWindow...
Available only in pro version	*	
Available only in pro version	*	

Name	Type	Data	Info

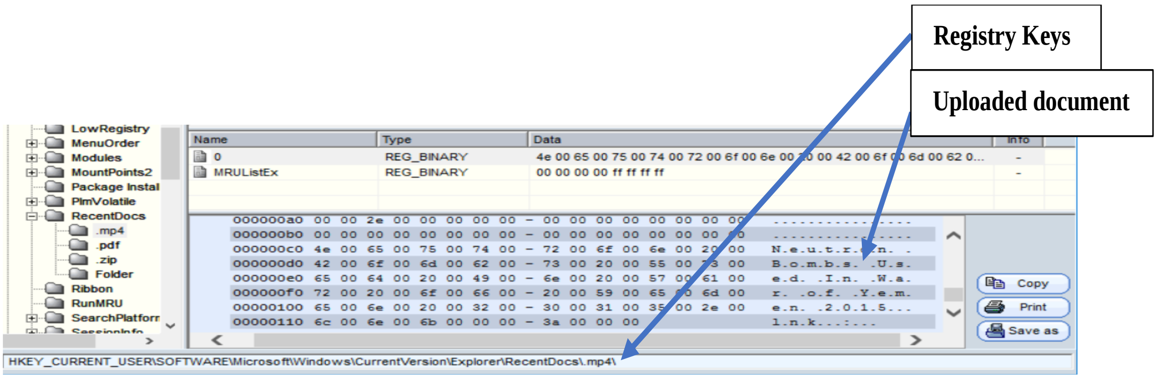
Key HKEY_CLASSES_ROOT\

Figure 5. Artifacts related IDrive installation



Key HKEY_LOCAL_MACHINE\SOFTWARE\IDRIVEW\pstadesina@outlook.com\

Figure 6. Artifacts related to login credential to the IDrive cloud storage

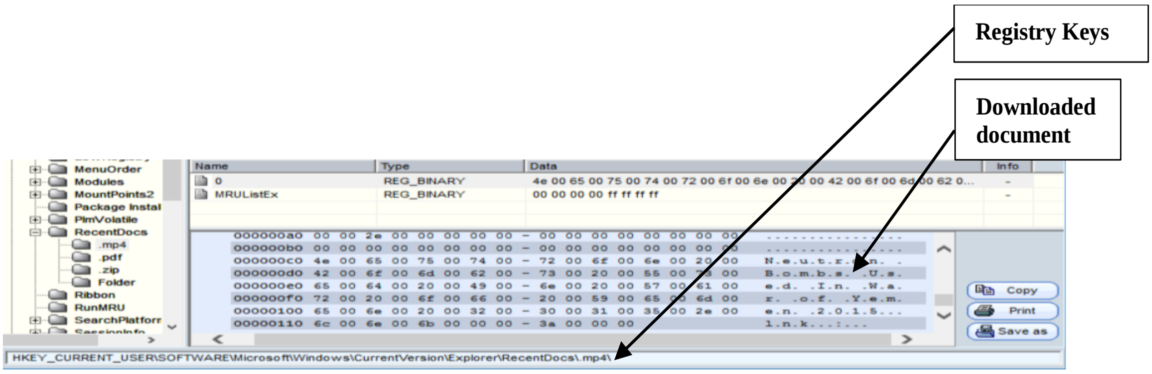


Name	Type	Data	Info
0	REG_BINARY	4e 00 65 00 75 00 74 00 72 00 6f 00 6e 00 20 00 42 00 6f 00 6d 00 62 0...	-
MRUListEx	REG_BINARY	00 00 00 00 ff ff ff ff	-

```
000000a0  00 00 2e 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ................
000000b0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ................
000000c0  4e 00 65 00 75 00 74 00 - 72 00 6f 00 6e 00 20 00   N.e.u.t.r.o.n. .
000000d0  42 00 6f 00 6d 00 62 00 - 73 00 20 00 55 00 73 00   B.o.m.b.s. .U.s.
000000e0  65 00 64 00 20 00 49 00 - 6e 00 20 00 57 00 61 00   e.d. .I.n. .W.a.
000000f0  72 00 20 00 6f 00 66 00 - 20 00 59 00 65 00 6d 00   r. .o.f. .Y.e.m.
00000100  65 00 6e 00 20 00 32 00 - 30 00 31 00 35 00 2e 00   e.n. .2.0.1.5...
00000110  6c 00 6e 00 6b 00 00 00 - 3a 00 00 00               l.n.k...:...
```

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mp4\

Figure 7. Artifacts related to the upload operation from windows 10 device to the IDrive cloud storage


Registry Keys

Downloaded document

Name	Type	Data	Info
0	REG_BINARY	4e 00 65 00 75 00 74 00 72 00 6f 00 6e 00 20 00 42 00 6f 00 6d 00 62 0...	-
MRUListEx	REG_BINARY	00 00 00 00 ff ff ff ff	-

```
000000a0  00 00 2e 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ................
000000b0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ................
000000c0  4e 00 65 00 75 00 74 00 - 72 00 6f 00 6e 00 20 00   N.e.u.t.r.o.n. .
000000d0  42 00 6f 00 6d 00 62 00 - 73 00 20 00 55 00 73 00   B.o.m.b.s. .U.s.
000000e0  65 00 64 00 20 00 49 00 - 6e 00 20 00 57 00 61 00   e.d. .I.n. .W.a.
000000f0  72 00 20 00 6f 00 66 00 - 20 00 59 00 65 00 6d 00   r. .o.f. .Y.e.m.
00000100  65 00 6e 00 20 00 32 00 - 30 00 31 00 35 00 2e 00   e.n. .2.0.1.5...
00000110  6c 00 6e 00 6b 00 00 00 - 3a 00 00 00               l.n.k...:...
```

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mp4\

Figure 8. Artifacts related to the download operation from IDrive cloud storage to the windows 10 device

3.2.5. Results presentation

The experiment with the registry analysis on iDrive cloud storage when windows 10 device accessed the cloud storage revealed the user’s behavior. The extracted or identified artifacts can be categorized based on 5Ws1H approach (what, who, where, why, when and how). This categorization can be used to present the forensic expression of the investigation and also illustrate the holistic view of the activities in relation to the cloud storage usage.

The identified artifacts in this research paper were categorized based on the principle of 5Ws1H as presented in Table 4. In Table 4, the WHAT represented the particular cloud storage that the investigator identified during the forensic analysis (iDrive), and the operations that were investigated (installation, upload, download, deletion and uninstallation operations). The WHO presented the account used to access the cloud storage (pstadesina@outlook.com) as identified during the analysis. The WHERE identified the path location on the device where the cloud storage was installed on. The WHY presented the assumed reason why the user carried out the operations on the cloud storage (all the datasets identified showed that the user was interested in terrorism materials (assumed reason). The HOW presented the approach the user used to access the cloud storage (client installation of the iDrive). The WHEN showed the day and time when the operations were carried out (In this experiment, no registry key was identified to hold these values). The categorized artifacts can be expressed using the 5Ws1H forensic expression to present the results of the identified artifacts as related to forensic investigation.

Table 4. Categorization of the identified artifacts based on 5Ws1H approach

The 5Ws1H of forensic investigation	Description	Instance (s)
What	Cloud Storage accessed with the Windows 10 device What are various operations performed on the Cloud Storage	iDrive instances found on registry keys Installation, Upload, Download, Deletion and Uninstallation operations.
Who	Credential that accessed the Cloud Storage	pstadesina@outlook.com
Where	the installation paths of the installed Cloud Storage	C:\ProgramFiles(x86)\IDriveWindows
Why	The assumed reason why the operations were performed	The nature of the recovered documents/files(datasets) revealed the interest of the user; the datasets discovered during the upload, download and uninstallation activities carried out on the Windows 10 device are terrorists’ materials which the user was working on. If the user is not interested in such activities, illegal files should not be found on his device.
How	The mode of accessing the storage	Client installation of the iDrive
When	The time of the operations	None

4. CONCLUSION

In this paper, the registry of a windows 10 device was forensically examined to identify relevant artifacts that were related to the usage of iDrive cloud storage when used with windows 10 device. The results showed that registry keys hold valuable forensic artifacts that are related to the usage of iDrive Cloud Storage when Windows 10 device is used. The extracted artifacts were also categorized based on the 5Ws1H approach to present the results of the investigation in such a way to assist forensic investigators to provide holistic and accurate evidence of the investigation. The study shows that the footprints of cloud storage activities can be forensically extracted from the digital devices that was used to access it, the extracted artifacts can also be reconstructed to determine the manner or patterns of its usage to determine the malicious usage. The study also shows that valuable artifacts can be obtained from digital devices without necessarily obtain the raw data or log from the concerned cloud service provide. The research enhances the efficiency of client forensics and crime investigation on cloud storages which can be extended to other digital devices and cloud storages to determine any form of malicious usages.

REFERENCES

[1] M. Attaran, "Cloud Computing Technology: Leveraging the Power of The Internet to Improve Business Performance," *Journal of International Technology and Information Management*, vol. 26, no. 1, pp. 112–137, 2017.

[2] R. Bahaweres and N. Santo, "Cloud Based Drive Forensic and DDoS Analysis on Seafile as Case Study," *Journal of Physics: Conference Series*, vol. 801, no. 012055, pp. 1-9, 2017, doi: 10.1088/17426596/801/1/012055.

[3] P. M. Mell and T. Grance, "The NIST Definition of Cloud Computing," *Special Publication (NIST SP) - 800-145*, 2018. [Online] Available: https://www.nist.gov/publications/nist-definition-cloud-computing.

[4] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," Security and Communication Networks, *Security and Communication Networks*, vol. 9, no. 18, pp. 6285-6314, 2016, doi: 10.1002/sec.1688.

[5] W.-F. Hsien, C.-C. Yang, and M.-S. Hwang, "A Survey of Public Auditing for Secure Data Storage in Cloud Computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016, [Online] Available: http://ijns.jalaxy.com.tw/contents/ijns-v18-n1/ijns-2016-v18-n1-p133-142.pdf.

[6] M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11-29, 2016, doi: 10.1016/j.jnca.2016.05.010.

[7] B. A. Alenizi, M. Humayun, and N. Jhanjhi, "Security and Privacy Issues in Cloud Computing," *Journal of Physics: Conference Series*, vol. 1979, no. 1, pp. 1-11, 2021, doi: 10.1088/1742-6596/1979/1/012038.

[8] P. Govindaraj, M. L. Shri, M. B. B. A. Malar, K. Santhi, and D. Mani, "Security algorithms in cloud computing: A review," *International Journal of Pure and Applied Mathematics*, vol. 117, pp. 85-92, 2017.

[9] S. Safavi, Z. Shukur, and R. Razali, "Reviews on Cybercrime Affecting Portable Devices," *Procedia Technology*, vol. 11, pp. 650-657, 2013, doi: 10.1016/j.protcy.2013.12.241.

[10] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191-1221, 2020, doi: 10.1109/COMST.2019.2962586.

[11] M. Shariati, A. Dehghantanha, and K.-K. R. Choo, "SugarSync forensic analysis," *Australian Journal of Forensic Sciences*, vol. 48, no. 1, pp. 95–117, 2015, doi: 10.1080/00450618.2015.1021379.

[12] H. Ali, "Forensically Important Artifacts in Windows Operating systems," *Digital Forensic Lead, Digital Forensic CoE*, [Online] Available: https://www.academia.edu/29746363/Forensically_Important_Artifacts_in_Windows_Operating_systems.

[13] F. Daryabar, A. Dehghantanha, and K.-K. R. Choo, "Cloud storage forensics: MEGA as a case study," *Australian Journal of Forensic Sciences*, vol. 49, no. 3, pp. 344-357, 2016, doi: 10.1080/00450618.2016.1153714.

[14] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, "CloudMe forensics: A case of big data forensic investigation," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 5, pp. 1-17, 2017, doi: 10.1002/cpe.4277.

[15] S. A. Razek, H. El-Fiqi, and I. Mahmoud, "Cloud Storage Forensics: Survey," *International Journal of Engineering Trends and Technology*, vol. 52, no. 1, pp. 22-35, 2017, doi: 10.14445/22315381/ijett-v52p205.

[16] M. Shariati, A. Dehghantanha1, B. Martini, and K.-K. R. Choo, "Ubuntu One Investigation: Detecting Evidences on Client Machines," arXiv:1807.10448pp. 429-446, 2015, doi: 10.1016/B978-0-12-801595-7.00019-7.

[17] S. Srinivasan, "Data Privacy Issues in Cloud Computing," *International Journal for Digital Society*, vol. 7, no. 4, pp. 1231-1237, 2016, doi: 10.20533/ijds.2040.2570.2016.0151.

[18] D. Quick and K.-K. R. Choo, "Google Drive: Forensic analysis of data remnants," *Journal of Network and Computer Applications*, vol. 40, pp. 179-193, 2014, doi: 10.1016/j.jnca.2013.09.016.

[19] B. Blakeley, C. Cooney, A. Dehghantanha and R. Aspin, "Cloud Storage Forensic: hubiC as a Case-Study," *IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, 2015, pp. 536-541, doi: 10.1109/CloudCom.2015.24.

[20] G. Satrya and S. Shin, "Proposed Method for Mobile Forensics Investigation Analysis of Remnant Data on Google Drive Client," *Journal of Internet Technology*, vol. 19, pp. 1741-1751, 2018, doi: 10.3966/160792642018111906011.

[21] T. Y. Yang, A. Dehghantanha, R. Choo, M. Conti, and T. Dargahi, "Forensic investigation of cooperative storage cloud service: Symform as a case study," *Journal of Forensic Sciences*, vol. 62, no. 3, pp. 641-654, 2016, [Online] Available: http://usir.salford.ac.uk/id/eprint/40496.

[22] S. H. Mohtasebi, A. Dehghantanha, and K.-K. R. Choo, "Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud, and pCloud," *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 205-246, 2017, [Online]. Available: https://arxiv.org/abs/1706.08042.

[23] G. B. Satrya, "Digital Forensics Study of a Cloud Storage Client: A Dropbox Artifact Analysis," *Journal Communication and Information Technology*, vol. 13, no. 2, pp. 57-66, 2019, doi: 10.21512/commit.v13i2.5781.

[24] S. Aggarwal *et al*., "A Targeted Data Extraction System for Mobile Devices," *Advances in Digital Forensics XV*, pp. 73-100, 2019, doi: 10.1007/978-3-030-28752-8_5.

[25] T. Rochmadi and D. Heksaputra, "Forensic Analysis in Cloud Storage with Live Forensics in Windows (Adrive Case Study)," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 4, pp. 292-297, 2019, doi: 10.17781/p002637.

[26] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, no. 2, pp. 71-80, 2012, doi: 10.1016/j.diin.2012.07.001.

BIOGRAPHIES OF AUTHORS

Adesoji A. Adesina is a faculty of the Department of Computer and Information Sciences at Covenant University Ota Ogun State, Nigeria. He holds a Bachelor Degree from Ladoke Akintola, Ogbomoso, Nigeria and a Masters Degree from Federal University of Technology, Akure, Nigeria. He is presently a PhD Student of Covenant University Ota Ogun State, Nigeria. His area of research interest includes incident response and cyber security management and digital forensics. He is a member of Nigerian Computer Society (NCS), Microsoft Certified Professional, Network+ Certified Professional and Security+ Certified Professional. He can be contacted at email: adesoji.adesina@stu.cu.edu.ng.

Professor Ayodele Ariyo Adebiyi is a faculty in the Department of Computer Science at Landmark University, Nigeria. He holds a B.Sc degree in Computer Science and MBA degree from University of Ilorin, Ilorin Nigeria. He had his M.Sc and Ph.D degree in Management Information System from Covenant University, Nigeria. His research interests include, application of soft computing techniques in solving real life problems, software engineering, electronic business, and mobile commerce research. He has published widely in local and international reputable journals. He is a member of Nigerian Computer Society (NCS), and the Computer Registration Council of Nigeria (CPN). He can be contacted at email: ayo.adebiyi@lmu.edu.ng.

Professor Charles K. Ayo holds a B.Sc, M.Sc, and Ph.D in Computer Science. His research interests include: mobile computing, e-Business, e-Government, e-Health and software engineering. Prof. Ayo is a member of a number of international research bodies and has being an External Examiner to a number of Nigerian and Foreign universities. He has supervised about 200 postgraduate projects and has several publications in scholarly journals and conference proceedings. He is well reputed Nationally and Internationally in the areas of application electronic and mobile technologies to governance, business, education and health among others. He can be contacted at email: charles.ayo@trinityuniversity.edu.ng.