

Detection and extraction of digital footprints from the iDrive cloud storage using web browser forensics analysis

Adesoji Adesina¹, Ayodele Adebisi², Charles Ayo³

¹Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria

²Department of Computer Science, College of Sciences, Landmark University, Omu-Aran, Nigeria

³Department of Computer and Information Sciences, Faculty of Basic Media and Applied Science, Trinity University, Yaba, Nigeria

Article Info

Article history:

Received Aug 10, 2021

Revised Jan 14, 2022

Accepted Feb 4, 2022

Keywords:

Artifacts
Cloud computing
Cloud forensic
Cloud storage
Cybercrimes
iDrive
Storage as a service

ABSTRACT

Storage as a service (STaaS) allows its subscribers the ability to access their stored data with the use of internet enabled digital devices at anywhere, anyplace and anytime. The easy accessibility of cloud storage with digital devices is one of the major benefits of cloud computing but this benefit can also be exploited by cybercriminals to perform various forms of malicious usages. During forensic investigation, forensic examiners are expected to provided evidence in relation to the malicious usages but the physical inaccessibility to the digital artifacts on the cloud servers, the difficulty in retrieving evidential artifacts from various cloud storage services and the difficulty in obtaining forensic logs from the concerned cloud service providers among other factors make it difficult to perform forensic investigations. This paper provided step by step experimental guidelines to extract digital artifacts from google chrome and internet explorer from Windows 10 personal computer using iDrive cloud storage as a case study. The study used Nirsoft forensic tool to locate the relevant forensic artifacts and an integrated conceptual digital forensic framework was adopted to carry out the investigation. This study increases the knowledge of client forensics using web browser analysis during cloud storage forensic investigation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adesina Adesoji

Department of Computer and Information Sciences, Covenant University

Ota Ogun State, Nigeria

Email: adesoji.adesina@stu.cu.edu.ng

1. INTRODUCTION

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) [1]. Storage as a service (STaaS) is an addition to these traditional service models [2] and is included in IaaS model of cloud [3], [4]. STaaS provides its subscribers the ability to access their data anywhere, anyplace and anytime on a wide range of Internet enabled devices as a result of its flexibility, affordability and portability [5]. These characteristics have positively impacted the cloud storage services popularity, usage and accelerated its adoption. Despite the benefits associated to the usage of cloud storage services, the security issues and the privacy of data in the cloud domain remain the major concerns to its subscribers, the forensics researchers and the practitioners [6]. The accessibility of cloud storage over the internet with the opportunity to store data online makes it susceptible to different malicious usages that include the utilization of the cloud storage to store and share illicit materials including child pornography and drug trafficking, sharing and distributing cyber terrorist materials [7]. When malicious activities involving cloud usages are

required, forensic examiners are required to conduct forensic investigations but there are various challenges involving the investigation of various malicious usages or criminal activities on cloud storages. These challenges have been identified as major challenges in the literature [8]-[10]. The difficulties include the inability to identify and recover digital evidence in a forensically sound manner on cloud storages [11], the dependence on the cloud service provider (CSP) to provide the relevant forensic logs which is difficult to obtain as a result of privacy and multi tenancy nature of cloud computing [12].

Despite the challenges associated with cloud forensics, when criminal acts or abuse of cloud storage takes place, it is necessary to carry out forensic investigation on cloud storages usages. Clients forensics investigation can be explored to obtain relevant forensic artifacts in respect of cloud storage usage. The investigation process in clients forensics include identifying, extracting, analyzing of forensic footprints (artifacts) from digital devices in relation to the malicious usages on cloud storage. Digital devices such as personal computer, tablets and smartphones are used to access cloud storage such as iDrive iCloud, Google Drive, OneDrive, relevant forensic footprints pertaining to the usages of the cloud storages are left on different locations on the devices which can be analyzed to detect the malicious usages [13]-[15]. Web browser is one of the locations that can be examined to investigate cybercrimes on digital devices because of its ability to provide wealth of information that pertains to the usage of web browser activities. Every step or action taken with the use of web browser that includes the web sites visited, the time of visit, the frequency of the access, files accessed, files downloaded and uploaded can be reconstructed to paint the clearer picture of the malicious usage [16]-[18].

This paper explores different artifacts created and retained on a Windows 10 digital device that can be extracted from the logs on Google Chrome and Internet Explorer web browsers when different activities including accessing, downloading and uploading of data sets on iDrive Cloud storage are carried out. iDrive cloud storage offers various forms of capabilities including online backup functionalities on wide range of digital devices which can be abused by the cybercriminals while Google Chrome and Internet Explorers were recorded as one of the highest used web browsers [19]. Forensic analysis of Web Browsers 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 other cloud storages. The results of the investigations in this study show that relevant forensic footprints of cloud storage usages can be obtained from the logs of web browsers. This study increases the knowledge of client forensics in relation to cloud storage usages and the significance of web browser analysis during digital investigations.

Research in literatures illustrate how forensic artifacts can be obtained from the web browsers of digital devices. Forensic analysis in [20] discovered the residual artifacts from the private and portable web browsing sessions on artifact extractions from Google Chrome, Mozilla Firefox, Apple safari and Internet Explore. Each of the web browsers under the investigations was forensically analyzed with different forensic tools to extract the relevant artifacts to establish an affirmative link between the user and the session. An experimental setup was proposed with the use of different hardware, software with the use of forensic tools. The results of the investigation showed that most of the recovered artifacts were discovered in random access memory (RAM), slack or free space and in forensic directories [21]. Investigated the forensic footprints that were left behind after the use of portable Google Chrome browser on Windows 7 operating system. The forensic stages employed are detection of incidence, evidence preservation, data acquisition, data analysis and reporting. Their approach delved deeper into Portable web browser to provide more forensic artifacts. The paper also presented an efficient forensic solution by reconstructing portable web browsing history to establish an affirmative link between a user and his portable web browsing activities which can serve as evidence that can be admissible in the court of law [22]. Analyzed and collected forensic artifacts that were related to internet activities from Google Chrome web browser on Windows operating systems. The locations examined to retrieve forensic artifacts included the browsing history, cookies, login data, topsides, shortcuts, user profile, prefetch file and RAM dump. The research provided guides on how different forensic techniques can be applied to obtain more robust digital artifacts from the different forensic web browser locations. Part of the artifacts extracted included the last accessed date and time of Google Chrome, search items, visited URLs, and how deleted items can be recovered [23]. Provided solutions to the extraction of forensic data from the RAM on a running system using live forensic analysis method. The authors used three stages of investigation that comprises of pro analysis, analysis and post analysis to detect digital evidence from the Internet Explorer, Google Chrome, Mozilla Firefox and Browzar web browser [24]. Illustrated how to carry out forensics analysis of data structures that were used by popular web browsers such as Chrome, Opera, Mozilla Firefox, and Dolphin on Android and how to acquire forensic artifacts from the web browsers. AndroKit forensic tool was introduced to acquire and analyze forensic evidence. The authors concluded that AndroKit has the capability to provide advance forensic data acquisition and analysis features that included flashing stock recovery and custom query execution. Jadhav and Meshram [25] the authors proposed a framework to detect the suspicious users' activities on the artifacts extracted from the web browser log files of Firefox, Google Chrome, Internet Explorer and Opera. Their implementation results showed the different

artifacts that were extracted during the analysis of cookies, analysis of downloaded history, analysis of browser history, analysis of website hosts data, analysis of searched keywords. The proposed framework component included the sources, evidence extraction and cleaning process, extracted evidence, evidence identification, arrange evidence in order, analyze all evidence, suspicious evidence and report generation. [26] provided the general review of web browsers attributes in different environments that included normal, private and portable mode of browsing, their limitations and the associated tools to perform forensic investigations. It was noted that the artifacts recovered in the private browsing sessions were less significant than in the public browsing sessions.

Mahlous and Mahlous [27] the authors setup a set of experiments that comprised of a live memory analysis of RAM and a post-mortem analysis to examine the artifacts that are retrievable from Brave web browser on Windows 10 device. Brave's privacy browsing mode was investigated to determine its privacy-preserving and forensic data acquisition. The artifacts' locations and the type of evidence available through live and post-mortem state analysis were documented. The authors concluded that live memory analysis of RAM provided more relevant artifacts compared to a post-mortem analysis. In the papers reviewed relevant forensic artifacts were examined but the different analysis were not linked to other public cloud storages like iDrive. Furthermore, the step-by-step procedures with good guidelines to assist during forensic investigations were not properly presented.

2. RESEARCH METHOD

The activity workflow process that guided in detecting relevant forensic artifacts from the web browsers (Google Chrome and Internet Explorer) on Windows 10 device examined in this research is depicted in Figure 1. The process comprises of the experimental setup, forensic analysis setup, forensic analysis and results presentation. It detailed the tool and the procedures employed to extract various artifacts from the Google Chrome and Internet Explorer on Windows 10 client device that accessed iDrive cloud storage.



Figure 1. Process workflow

2.1. Experimental setup

The experimental setup to detect the relevant artifacts with the traces of iDrive usage from the logs of Google Chrome and Internet Explorer on Windows10 digital device is discussed. The experimental setup for this research study consists of a virtual machine (host) that was setup 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 total of 10 virtual machines (VMs) was built on the virtual host to carry out various activities that can be carried out on Windows 10 device while using the web browsers to access iDrive cloud storage.

The 10 VMs represent the different physical systems to simulate series of life scenarios (common activities) of using any cloud storage. The experiments were carried out with datasets in different formats (Word Documents, portable document formats (pdf) and video clips) that are related to terrorism activities downloaded from different internet websites. Nirsoft freeware forensic tool (Web Browser History Viewer, IE PassView, OpenSaveFilesView and ChromeHistoryView) version 1.23.24 was used and installed on each VM to detect different artifacts on each virtual machine under investigation, Google Chrome version 78.0.3904.108 was downloaded and manually installed.

2.2. Forensic analysis setup

To perform Windows 10 Web-based experiment in this study, ten virtual machines were setup (VM1-VM10). Each of the VMs (VM1-VM10) as shown in Figure 2 and Table 1 represents the different common activities that can be carried out on the cloud storage (access, upload, download and deletion) with any type of web browser.

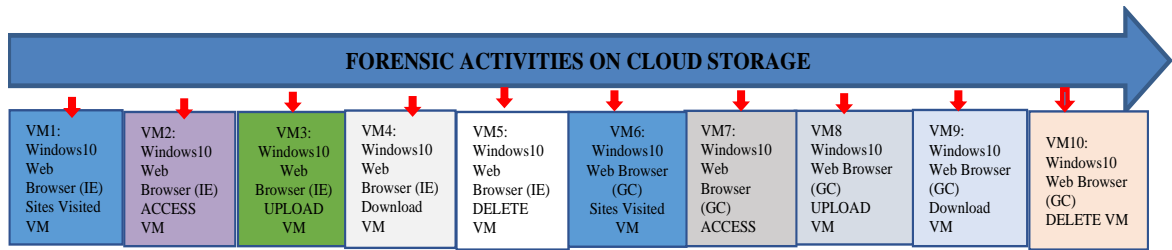


Figure 2. Activities on Windows 10 device with the use of Internet Explorer and Google Chrome web browsers

Table 1. Windows web browser-Based VM activities on the cloud storages

Windows10 Web Browser ACCESS VM	Windows10 Web Browser UPLOAD VM	Windows10 Web Browser UPLOAD VM	Windows 10 Web Browser DOWNLOAD VM	Windows 10 Web Browser DELETE VM
VM1: using IE to examine the different web sites visited to identify the cloud storage accessed	VM2: using IE to determine the relevant artifacts related to the credentials that were used to access IDRIVE cloud storage on Windows 10 device	VM3: using IE to determine the relevant artifacts that are related to the upload operation on IDRIVE cloud storage on Windows 10 device	VM4: using IE to determine the relevant artifacts that are related to the download operation on IDRIVE cloud storage on Windows 10 device	VM5: using IE to determine the relevant artifacts that are related to the delete operation on IDRIVE cloud storage on Windows 10 device
VM6: using GC to examine the different web sites visited to identify the cloud storage visited	VM7: using GC to determine the relevant artifacts related to the credentials that were used to access IDRIVE cloud storage on Windows 10 device	VM8: using GC to determine the relevant artifacts that are related to the upload operation on IDRIVE cloud storage on Windows 10 device	VM9: using GC to determine the relevant artifacts that are related to the download operation on IDRIVE cloud storage on Windows 10 device	VM10: using GC to determine the relevant artifacts that are related to the delete operation on IDRIVE cloud storage on Windows 10 device

2.3. Implementation procedures

The procedures employed to analysis Web browser forensic analysis to detect the traces of iDrive cloud storage on Windows 10 device involved the installation of Nirsoft forensic tool. Nirsoft freeware was installed on each of the VM (VM1-VM10). Nirsoft utilities (downloaded from Nirsoft.com) used during the forensic analysis include the WebBrowserHistoryViwer, IEPassViewer and OpenSavedFilesViewer.

In this procedure, useful artifacts were retrieved using the Nirsoft forensic tools. These forensic artifacts provided useful information concerning the usage of the web browsers. The extracted artifacts related to iDrive cloud storage usages from the Web browser of Google Chrome and Internet Explorer from Windows 10 device include the different web sites visited and the credentials (the username and password) are discussed in Experiment.

2.3.1. Experiment 1

This experiment was performed on VM1 to examine the different websites that a user visited on the Windows 10 device with the Internet Explorer web browser. Web Browser History Viewer utility embedded in Nirsoft package was used to identify different websites visited with IE. The interface of the Web Browser History Viewer that showed result of the analysis on VM1 is showing in Figure 3.

2.3.2. Experiment 2

This experiment was performed on VM2 to examine the credential (username and the password) used to access the iDrive cloud storage when Internet Explorer web browser was used to access the iDrive. IE PassView utility embedded in Nirsoft package was used to reveal the credential(s) used to access the iDrive with Internet Explorer. The interface of the experiment performed on VM2 that revealed the username and password that accessed the iDrive are captured in Figure 4.

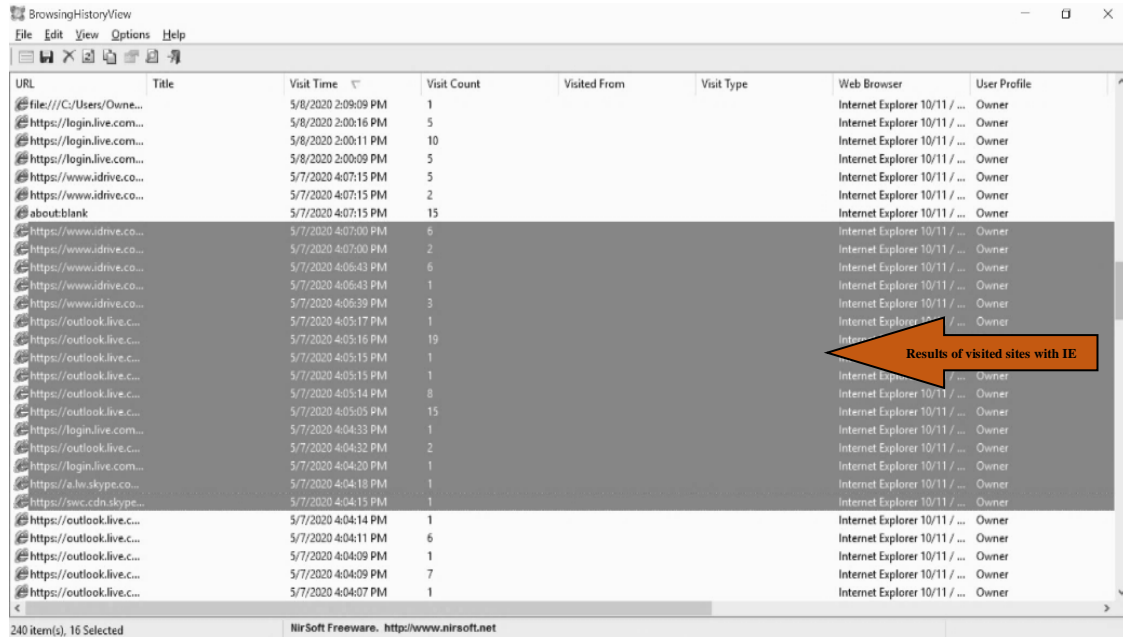


Figure 3. Interface showing different web sites visited including idrive.com on VM1

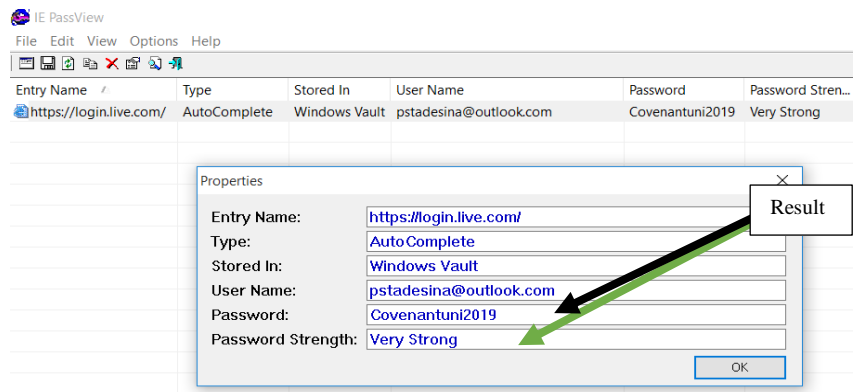


Figure 4. The extracted username and password that accessed iDrive in IE

2.3.3. Experiment 3

This experiment was performed on VM3 to examine the uploaded files from the Windows 10 PC to the iDrive cloud storage. OpenedFilesView utility embedded in Nirsoft package was used to extract the uploaded files from VM3. The interface on the OpenSafeFilesView revealing the uploaded files is shown in Figure 5.

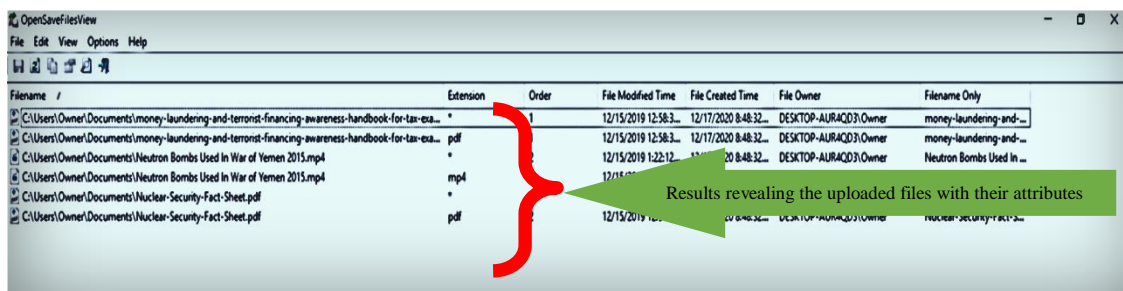


Figure 5. OpenFilesView forensic tool revealing the uploaded documents and the paths in IE

2.3.4. Experiment 4

This experiment was performed on VM4 to examine the downloaded files from the iDrive cloud storage to the Windows 10 PC. OpenedFilesView Utility was used to extract the downloaded files. The same interface with Figure 5 was observed, then the username and password obtained in experiment 3 was used to view the log on iDrive. The interface of the viewed log on iDrive revealing the downloaded files is captured in Figure 6.

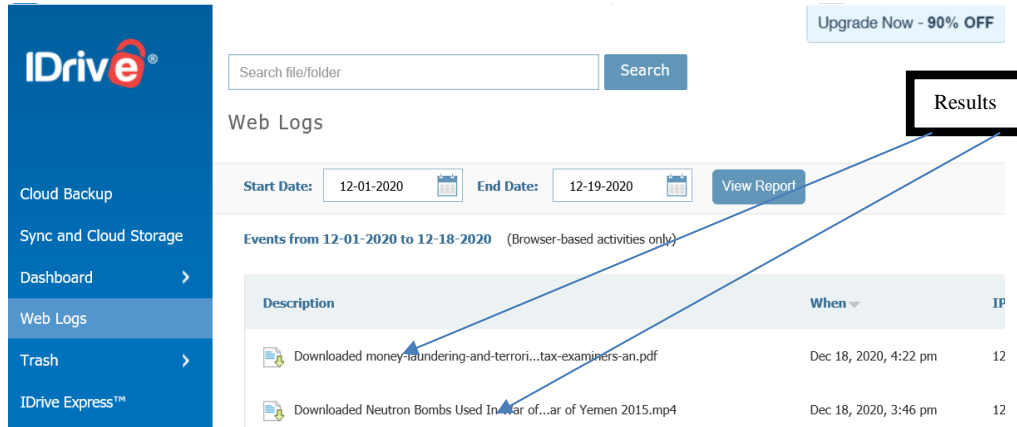


Figure 6. Web logs on iDrive showing the download documents

2.3.5. Experiment 5

This experiment was performed on VM5 to examine the retrieval of deleted files from the iDrive. None of the Nirsoft utilities used employed was able to retrieve the deleted files but the web log interface of the idrive recorded the deleted activity when the username and password extracted in experiment 3 was used. The interface of the viewed log on iDrive revealing the deleted files is shown in Figure 7.

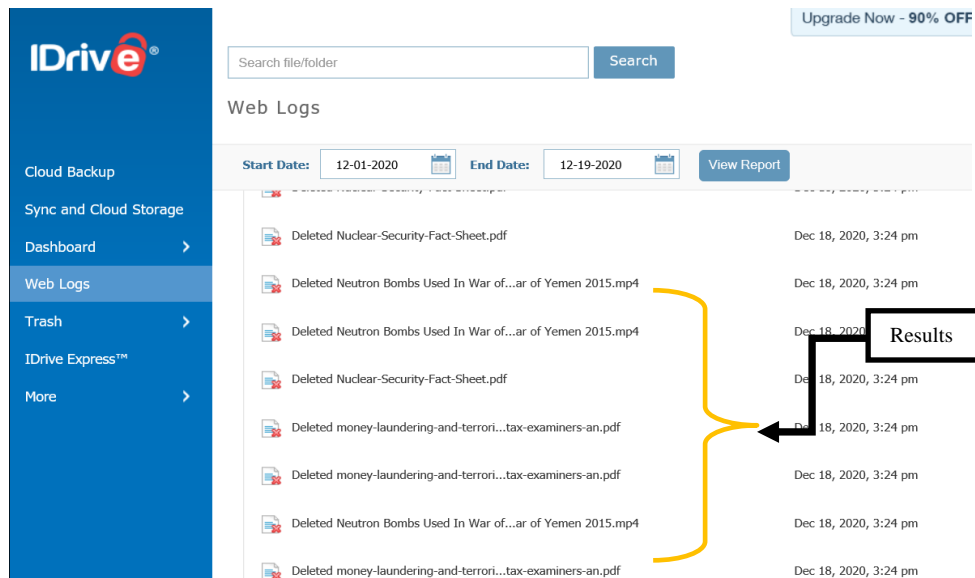


Figure 7. Web logs on iDrive showing the deleted files

2.3.6. Experiment 6

This experiment was performed on VM6 to examine the different websites that a user visited on the Windows 10 device with the Google Chrome web browser. ChromeHistoryView utility embedded in Nirsoft package was used to identify different websites visited. The interface of the experiment performed on VM6 showing the different websites visited with the use of Chrome History View forensic tool is presented in Figure 8.

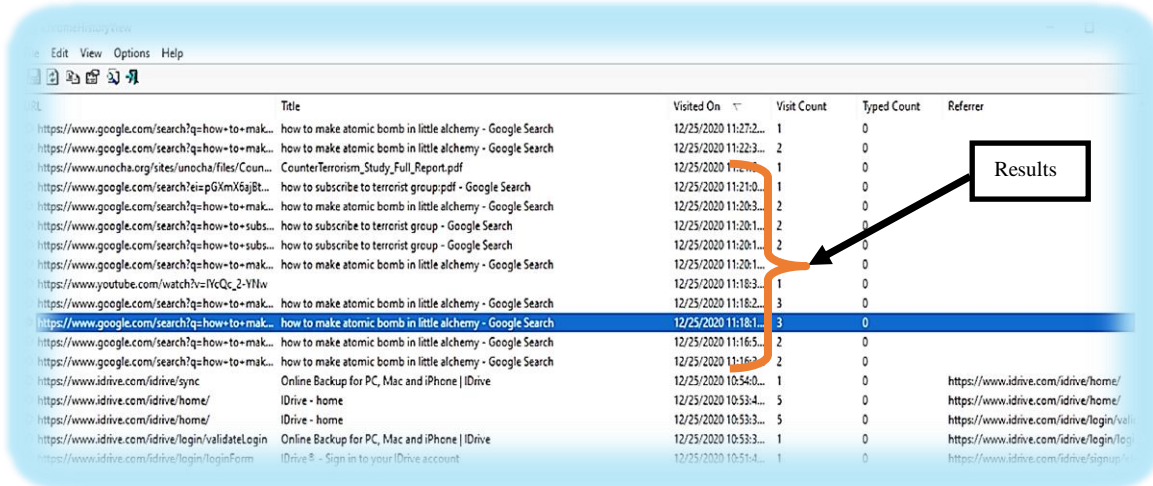


Figure 8. Interface showing different web sites visited on VM6 with Browser History Viewer in GC

2.3.7. Experiment 7

This experiment was performed on VM7 to examine the credential (username and the password) used to access the iDrive cloud storage when Google Chrome web browser was used. Chrome Pass utility in Nirsoft package was used to reveal the credential used to access the IDRIVE with Google Chrome. The interfaces of the experiment performed on VM7 revealing the username and password that accessed the IDRIVE is captured in Figure 9.

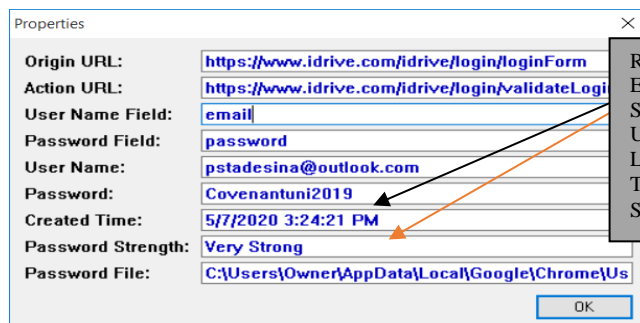


Figure 9. Extracting username and password that accessed iDrive using Chrome Pass in GC

2.3.8. Experiment 8

This experiment was performed on VM8 to examine the uploaded files from the Windows 10 PC to the iDrive cloud storage with Google Chrome web browser. OpenedFilesView utility in Nirsoft package was used to extract the uploaded documents. The interface of the experiment performed on VM8 revealing the uploaded documents is presented in Figure 10.

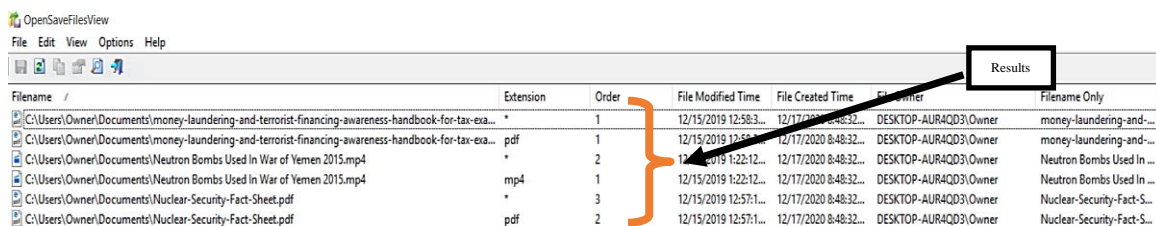


Figure 10. Open files view revealing the uploaded documents and the paths in GC

2.3.9. Experiment 9

This experiment was performed on VM9 to examine the downloaded files from the iDrive cloud storage to the Windows 10 PC when Google Chrome was used. BrowserDownloadView utility embedded in Nirsoft package was used to extract the downloaded documents. The interface of the experiment performed on VM9 revealing the downloaded documents is presented Figure 11.

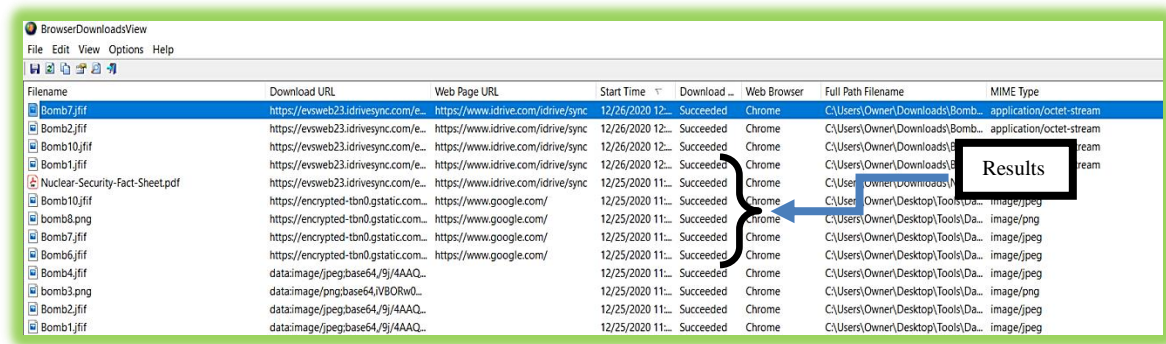


Figure 11. The extracted downloaded files with browser download view

2.3.10. Experiment 10

This experiment was performed on VM10 to examine the retrieval of deleted files from the iDrive when Google Chrome was used to access the iDrive cloud storage. None of the Nirsoft utilities used was able to retrieve the deleted files. The extracted account name and password retrieved in Experiment 6 was used to access iDrive cloud storage. The uploaded documents in experiment 8 were deleted with the utility on the iDrive environment. The web log was viewed to see if the deletion operation was recorded as shown in Figure 12 The interface of the experiment performed on VM10 revealing the deleted documents is shown in Figure 12.

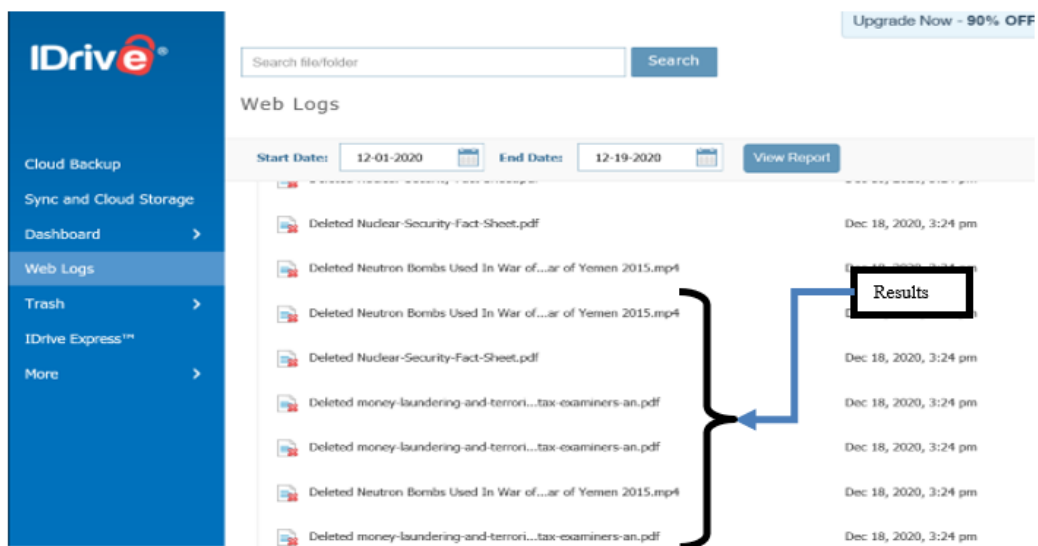


Figure 12. Web Logs interface showing the deleted items from the iDrive trash

3. EXPERIMENTAL RESULTS AND DISCUSSION

The results of the forensic analysis in this research shows that relevant residual artifacts related to the different operation carried out on iDrive cloud storage are retrievable from Google Chrome and Internet Explorer web browsers. Experimental guidelines were presented that captured relevant screenshots of retrievable artifacts from iDrive platform using the Nirsoft freeware forensic tool. The study analyzed the iDrive on Windows 10 operating system considering the basic operations that cloud users undertake on cloud

storage (Web sites visit, Login, Upload, Download, Deletion operations). The experiments showed that the different web sites visited, the credentials that were used to access the web site (cloud storage) and different files operations can be forensically extracted with the use of appropriate forensic tools to reconstruct any form of cybercrimes to determine the when, what, why, when, who and the how of digital forensic investigations that can provide valid evidence related to the abuse or malicious usages of cloud storage.

4. CONCLUSION

In this research study, the relevant residual forensic artifacts from Windows 10 device that are retrievable from Google Chrome and Internet Explorer web browsers were presented using iDrive cloud storage a case study. Experimental guidelines were provided that captured relevant screenshots of retrievable artifacts from iDrive platform using the Nirsoft freeware forensic tool. The study analyzed different iDrive artifacts on Windows 10 devices when the device was used to access iDrive cloud storage considering the basic operations that cloud users undertake on cloud storage (including the Web sites visit, Login, Upload, Download, Deletion operations). The experiments showed that the web sites visited, the credentials that were used to access the web site (cloud storage) and different files operations can be forensically extracted to reconstruct any form of cybercrimes to determine the usages of the cloud storage. The research findings showed that a single forensic tool may not be sufficient to extract all the required artifacts to fully reconstruct cybercrimes, more than one tools may be necessary to provide all the necessary details to proof the cybercrime activities. Extending the presented approach in this work to other web browsers like Safari on iPhone, SamSung Internet on SamSung devices and other popular web browsers on other digital devices running on any operating systems like Android, iOS, Ubuntu and MAC OS will be of great interest to further research on clients forensics with respect to the cloud storage usages. Considering the legal and privacy issues of conducting digital forensics analysis on personally own devices and cloud storage would be of great importance in conducting forensic analysis on real life cases.




REFERENCES

- [1] M. Attaran, "Cloud computing technology: leveraging the power of the internet to improve business performance.," *Journal of International Technology & Information Management*, vol. 26, no. 1, pp. 112–137, 2017, [Online]. Available: <http://login.library.sheridanc.on.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=128288921&site=ehost-live&scope=site>.
- [2] R. B. Bahaweres, N. B. Santo, and A. S. Ningsih, "Cloud based drive forensic and DDoS analysis on seafile as case study," *Journal of Physics: Conference Series*, vol. 801, no. 1, p. 012055, Jan. 2017, doi: 10.1088/1742-6596/801/1/012055.
- [3] P. Mell and T. Grance, "The NIST definition of cloud computing," in *Application Performance Management (APM) in the Digital Enterprise*, Elsevier, 2017, pp. 267–269.
- [4] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," *Security and Communication Networks*, vol. 9, no. 18, pp. 6285–6314, Dec. 2016, doi: 10.1002/sec.1688.
- [5] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, T. Dargahi, and M. Conti, "Forensic investigation of cooperative storage cloud service: symform as a case study," *Journal of Forensic Sciences*, vol. 62, no. 3, pp. 641–654, May 2017, doi: 10.1111/1556-4029.13271.
- [6] Y. Shi, "Data security and privacy protection in public cloud," in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, Dec. 2019, pp. 4812–4819, doi: 10.1109/BigData.2018.8622531.
- [7] F. Neagu and A. Savu, "Comparative study on CyberTerrorism," *Knowledge Horizons. Economics*, vol. 11, no. 1, pp. 93–98, 2019.
- [8] T. Raja Sree and S. Mary Saira Bhanu, "Data collection techniques for forensic investigation in cloud," in *Digital Forensic Science*, IntechOpen, 2020.
- [9] E. M. Lopez, S. Y. Moon, and J. H. Park, "Scenario-based digital forensics challenges in cloud computing," *Symmetry*, vol. 8, no. 10, p. 107, Oct. 2016, doi: 10.3390/sym8100107.
- [10] M. Y. Arafat, B. Mondal, and S. Rani, "Technical challenges of cloud forensics and suggested solutions," *International Journal of Scientific and Engineering Research*, vol. 8, no. 8, pp. 1142–1149, Aug. 2017, doi: 10.14299/ijser.2017.08.004.
- [11] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, "Digital evidence in cloud computing systems," *Computer Law and Security Review*, vol. 26, no. 3, pp. 304–308, May 2010, doi: 10.1016/j.clsr.2010.03.002.
- [12] B. Martini and K. K. R. Choo, "Cloud storage forensics: OwnCloud as a case study," *Digital Investigation*, vol. 10, no. 4, pp. 287–299, Dec. 2013, doi: 10.1016/j.diin.2013.08.005.
- [13] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digital Investigation*, vol. 9, no. 2, pp. 81–95, Nov. 2012, doi: 10.1016/j.diin.2012.05.015.
- [14] A. A. Abbasi, S. Saleem, and R. Zulqarnain, "Mobile forensic investigation of cloud storage applications," *NUST Journal of Engineering Sciences*, vol. 10, no. 1, pp. 30–396, 2017.
- [15] T. Z. Khairallah and J. Amman, "Cloud drives forensic artifacts a google drive case," *Preprints*, 2019, doi: 10.20944/preprints201812.0345.v1.
- [16] E. Akbal, F. Güneş, and A. Akbal, "Digital forensic analyses of web browser records," *Journal of Software*, vol. 11, no. 7, pp. 631–637, Jul. 2016, doi: 10.17706/jsw.11.7.631-637.
- [17] C. Flowers, A. Mansour, and H. M. Al-Khateeb, "Web browser artefacts in private and portable modes: A forensic investigation," *International Journal of Electronic Security and Digital Forensics*, vol. 8, no. 2, pp. 99–117, 2016, doi: 10.1504/IJESDF.2016.075583.




- [18] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digital Investigation*, vol. 8, no. SUPPL., pp. S62–S70, Aug. 2011, doi: 10.1016/j.diin.2011.05.008.
- [19] W3C, "W3Counter: Global Web Stats - November 2014," Web Browser Market Share, 2014. <http://www.w3counter.com/globalstats.php?year=2014&month=11>.
- [20] D. J. Ohana and N. Shashidhar, "Do private and portable web browsers leave incriminating evidence? A forensic analysis of residual artifacts from private and portable web browsing sessions," in *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013*, May 2013, pp. 135–142, doi: 10.1109/SPW.2013.18.
- [21] E. D. and N. Meeran, "Forensic reconstruction and analysis of residual artifacts from portable web browser," *International Journal of Computer Applications*, vol. 128, no. 18, pp. 19–24, Oct. 2015, doi: 10.5120/ijca2015906741.
- [22] D. M. Rathod and D. Rathod, "Web browser forensics: Google Chrome," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, pp. 896–899, 2017, doi: 10.26483/ijarcs.v8i7.4433.
- [23] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live forensics for anti-forensics analysis on private portable web browser," *International Journal of Computer Applications*, vol. 164, no. 8, pp. 31–37, 2017, doi: 10.5120/ijca2017913717.
- [24] M. Asim, M. F. Amjad, W. Iqbal, H. Afzal, H. Abbas, and Y. Zhang, "AndroKit: A toolkit for forensics analysis of web browsers on android platform," *Future Generation Computer Systems*, vol. 94, pp. 781–794, May 2019, doi: 10.1016/j.future.2018.08.020.
- [25] M. R. Jadhav and B. B. Meshram, "Web browser forensics for detecting user activities," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 7, 2018, doi: 10.13140/RG.2.2.25857.51049.
- [26] A. Rasool and Z. Jalil, "A review of web browser forensic analysis tools and techniques," *Researchpedia Journal of Computing*, vol. 1, no. 1, pp. 15–21, 2020, [Online]. Available: <https://www.researchgate.net/publication/342338294>
- [27] A. R. Mahlous and H. Mahlous, "Private browsing forensic analysis: A case study of privacy preservation in the brave browser," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 6, pp. 294–306, Dec. 2020, doi: 10.22266/ijies2020.1231.26.

BIOGRAPHIES OF AUTHORS






Adesoji 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, Ogbomosho, 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). He can be contacted at email: adesoji.adesina@stu.cu.edu.ng.



Prof. Ayodele Adebisi    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.adebisi@lmu.edu.ng.



Prof. Charles 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.