Cloud Forensics: Dropbox and OneDrive as Case Study

Zaina AlSaed and Mahmoud Jazzar

Faculty of Graduate Studies
Palestine Technical University – Kadoorie
Tulkarm, P. O. Box 7, Palestine

Abstract—The increasing popularity of cloud computing controlled the adoption of cloud applications by variety of enterprises and individuals. This enlarged the scale of cloud storage usage rate. In addition, there was an essential need for robust methods of cloud forensics. Criminals could employ the cloud for their intentions by mistreating it as part of any suspicious activity. Inspectors look for any related evidence either within the cloud or the local system. The main objective of this paper is to highlight the relative artifacts of popular cloud service providers such as Microsoft's OneDrive and Dropbox. At this stage Dropbox and OneDrive desktop applications were monitored. After experimentation, traceable artifacts in both Dropbox and OneDrive applications were noted.

Keywords—Cloud forensics; Cloud storage; Digital forensics; OneDrive; Dropbox

1. INTRODUCTION

Cloud computing technologies continues to grow significantly popular among individual users and businesses. Cloud technology switches many cloud services in various forms in daily basis which motivate verity of exploitations and new form of attacks [1]. Users all over the globe benefit from cloud services when they use services like Google Drive, Dropbox, OneDrive, and EC2 instances by Amazon. The expansion in cloud computing adoption has emerged in an increasing call for investigating concerning cloud computing forensics. This has issued investigations for cloud software technologies. Cloud computing offers particular usage of digital means with a minimum resolution of administration [2], it uses virtual services that could be reached by public users as mean of resources [3]. According to NIST's description, there are five primary characteristics that define cloud services which mainly describes the cloud technology as an on-demand service, wide network access service, self-service, resource pooling service, with fast flexibility [4].

There are different kinds of clouds that are now implemented by cloud service providers. A cloud foundation that is maintained by a cloud service provider (CSP) is declared as a public one. The CSP is capable to handle the cloud while sharing and marketing the cloud resources to other firms [5]. Whereas in private clouds infrastructure is for the particular use of one organization exclusively. Thus, the organization maintains the cloud and utilizes the resources. Generally, the company is liable for securing the cloud. A community cloud in which the infrastructure is held and managed by numerous groups. This sort of cloud service is usually managed by a company or third party [5]. The greatest hybrid clouds join public cloud and the private cloud. Despite the hybrid cloud handles varied kinds of clouds, each of them still operates individually [5]. Besides its wide usage, cloud computing technology still a problem to understand which make it term to be discussed in many kinds of research. Criminal attack cloud services, intruders may drip secret data from users by exploiting cloud storage that enables to save data like images and obtain them by endpoint tools.

The safety of cloud computing is highly important point that necessitates numerous further investigations. From forensic prospect, there are many topics to discuss such as the analysis of the cloud applying common digital forensic tools. An example of such issues, throughout conventional digital forensic case, all records that are stored are analyzed beside the whole file system. However, it cannot be counted as suitable model for the cloud-base as the flexibility of merged storage may cause conflict.

Digital forensics has been employed widely in the digital criminal investigation processes during the past three decades. While particular general description is absent for cloud forensics, numerous researchers appear to admit that it can be presented as connection between cloud computing technology and digital forensic processes [6]. Data gained from cloud forensics need to meet identical terms to traditional data of evidence requirements. Some of the problems in cloud forensics may develop from meeting such specifications. Cloud forensics is prominent category of network forensics, which suggests the post-incident study of techniques with virtualization, scattered processing, multi-tenant, and mobility computations. Researchers in [7] classify many difficulties linked to cloud forensics. These involve the interdependence of forensically-important evidence on the cloud methods and model, extensive sizes of data, exclusive data forms, absence of supervision and warnings by hypervisors that manage virtual machines, in addition to concurrently executing virtual machine instances and inadequate methods and mechanisms created primarily for cloud forensic studies. The authors in this work discuss the challenges of using cloud technology by experimentation. Cloud computing is considered as challenging issue for forensic analysts and investigators. Information and data can be uploaded, opened, or transferred within several devices without leaving any evident proof. In this work, Microsoft OneDrive and Dropbox are case studies of cloud storage services that are investigated and the obtained results are discussed.

2. BACKGROUND

Cloud computing technology depends on three main key service deployments. First, Software-as-a-Service (SaaS) which permits users to utilize cloud service provider (CSP) employment operating on cloud-base setting. The second is Platform-as-a-Service (PaaS) which allows users to set up their applications applying programming tools and libraries that are maintained by the CSP. Finally, the Infrastructure-as-a-Service (IaaS) which gives clients the options to reserve, process, store data on several computing resources, including applications and multiple operating systems [7].

Cloud forensics sector represents category of network forensics that handles methods that discuss cloud computing systems [7]. For instance, data retrieval is unconventional in the SaaS and IaaS types. In SaaS, an inspector has to rely totally on the cloud service provider. While virtual machine images can be obtained from users in IaaS model.

Many procedures have been introduced to obtain forensic data from the cloud, such as remote evidence retrieval, control level acquisition, snapshot examination [8]. Researchers such as in [9] have gained different sorts of data from Amazon EC2 cloud running user instance stage utilizing conventional investigative tools like EnCase and FTK. Such data is classified into both volatile and non-volatile types. Similar software tools do not verify the originality of the acquired data. Researchers in [10] proposed FROST investigative tool, which can be combined to gather records from the OS that runs the VM; this procedure implies that the CSP is reliable. Zawoad et al. in [11] have created forensics-enabled, full and reliable cloud model. Hay and Nance [12] have also carried out active digital forensic investigations by virtual contemplation, which stands for processes that lets the VM or the hypervisor inspect the status of determined virtual machine. Besides, they produced a set of virtual self-analysis tools (VIX tools) for Xen. Back then, active (live) forensic toolkits have not been included by cloud providers. On the other hand, Snapshot technology allows cloud users to stop virtual machines from running in particular cases [13]. Snapshot features are supported by various hypervisors, (such as VMWare). To store frozen snapshot photo, it can be recovered by storing it to destination VM, keeping in mind which data regarding the ongoing situation of the VM can be saved. To decrease the required time and work associated with forensic examinations, inspectors have suggested the adoption of commands to automate data exchange and attack restoration [14],[15].

Liu et al. in [15] have built Prolog-based software and an anti-forensic tool, a vulnerability database to determine the validation of evidence and resolve the non-existing evidence because of the application of anti-forensic methods. However, these examination structures have not been for cloud environments. Authors in [17] held an experiment to test Dropbox on a Windows 7 OS. Similarly, in [17], the work addressed the same issues in addition to iOS. Taking the problem slightly and differently, forensics were done on cloud services on various OSs [18]. Moreover, researchers in [19] denoted the Microsoft SkyDrive forensics on both PCs and iOS.

3. METHOD

3.1 Experiment Outline

In this study, we have developed an investigation case created according to cloud operating practices. The primary aim is to discuss key features of various cloud storage applications to assist law enforcement and the digital forensic investigation process. Accordingly, it is essential to obtain all related artifacts generated, files or metadata of files uploaded, and regardless the files were deleted or not. We have chosen and examined two commonly-used Cloud Service Providers, Dropbox and OneDrive. Dropbox is a service that provides web-based file sharing as well as synchronization services. The peculiarity is the capability of automatic file synchronization over several devices. A need for Dropbox client is important to take place on devices that need to sync files. The client operates continually observing any log on the local system in the selected Dropbox folder and then sync with the cloud. Dropbox sponsors mixture of operating systems (Both mobile and desktop). Clients have the option to obtain their data whenever they want by any service linked to Dropbox. On the other hand, OneDrive is file-hosting service that provides variety of services such as personal cloud, file synchronization, online storage, and client software. OneDrive gathers files, all in single space by making designated place on the PC. The files of such contents are synced to the OneDrive servers and other systems that installed OneDrive, holding the alike files updated on all systems. This cloud service is accessible for Linux, macOS, and Microsoft Windows, as well as its availability on all smartphones and tablets.

CSPs are investigated to prove that possible evidence could be located in Internet cache, navigation history, temporary and log files, Web browser's cookies, and downloaded files. In this regard, we created a Windows 7 20GB virtual machine (VM) for Dropbox and for OneDrive. Then, we downloaded Sysinternals Process Monitor to observe and report any modifications that were done during use, from the beginning of installation to the uninstallation of cloud services. Hence, we proceeded with downloading and installing the cloud service. We observed outcomes from the registry activity and file system. After finishing the installation process, we collected the outcomes from the Process Monitor tool and powered off the VM. In addition, cloned Virtual Machine set to new location to save the original artifacts that were formed throughout the installation. To begin the experiment, we managed the test scenarios whose preparatory steps are connected to the cloud service and then creating an account. The following illustrate the procedure.

- Powering on the VM.
- Starting Process Monitor.
- Applying scenarios such as:
  - Setup.
  - Uploading Files.
  - Copying files.
  - Moving files.
  - Opening files.
  - Deleting files.
  - Unlinking the account.
  - Uninstallation.
- Saving the outcomes.
- Powering off the Virtual Machine.
- Copying the Virtual Machine to new folder again.

The deleted files from Dropbox were "test1.exe" and "welcome.pdf". Files named "dforensics.txt" and "drivetest.png" were deleted from the OneDrive folder. After we completed designing the VM, we applied FTK Imager 7.4.2 to create an E01 file for the VM. Accordingly, we held seven distinct images to analyze through FTK in addition to some CSV files observed by the Process Monitor software to inspect modifications done to both files and registry.

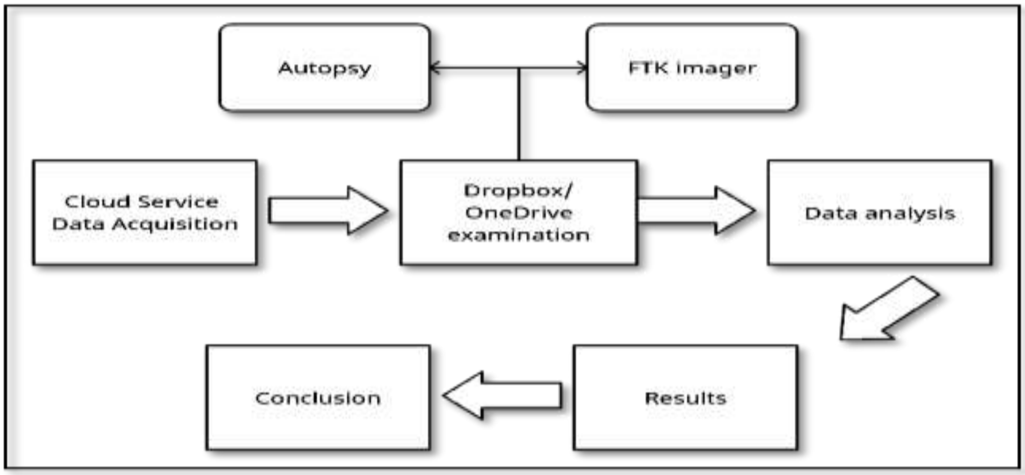

Fig. 1. *Experiment overview flowchart.*

3.2 Software Installed

- VMware Workstation 16.1.1
- Windows 7 64-bit
- Process Monitor v2.95
- Dropbox
- Microsoft OneDrive
- Autopsy 4.18.0
- FTK Imager 4.31.1

3.3 Dropbox Forensics

3.3.1 Data Gathering

The assembled data for this scheme combined CSV files obtained from Process Monitor and files from FTK. Figure 2 demonstrates the total amount of filtered files using the Process Monitor for Dropbox cloud service.

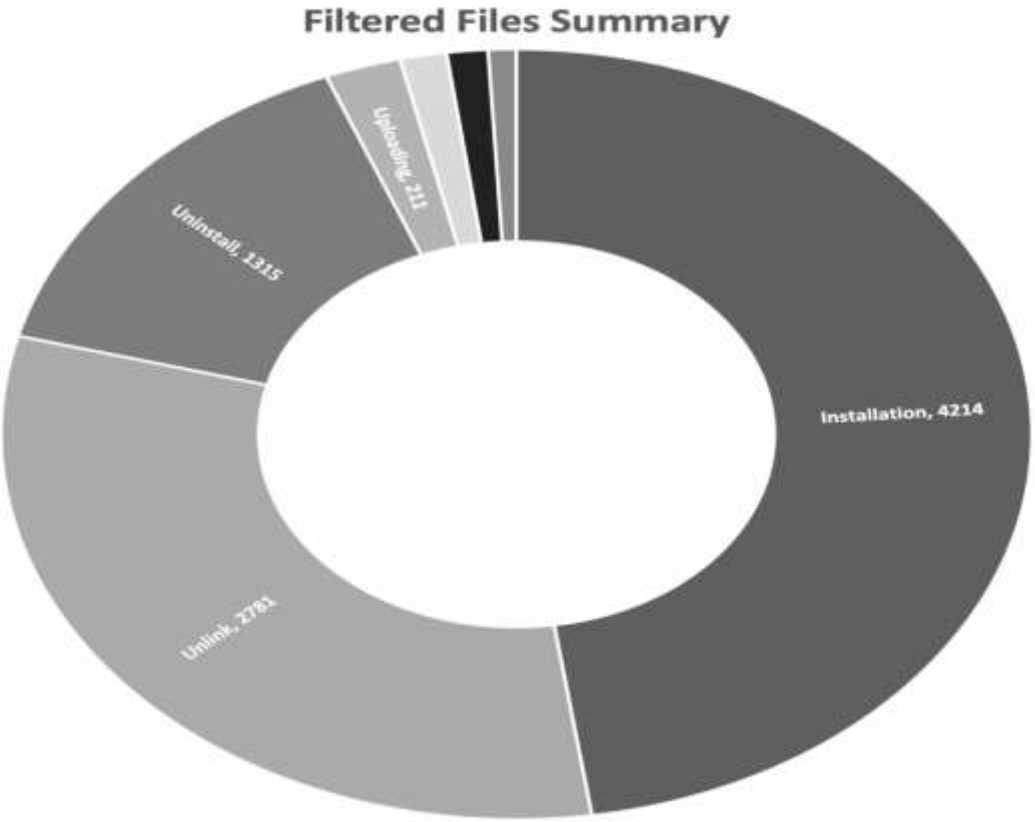

Fig. 2. *Dropbox Filtered Files Summary.*

3.3.2 Analysis

The investigation dataset was derived from CSV files generated and associated with the examination outcomes of FTK. We focused on analyzing data according to the path results, filtering using Excel, and the following:

1. Unique paths classified as:
   - File path.
   - Registry path.
2. To clarify the outcomes, files involve the word ‘Dropbox’ were only listed. This step was essential to demonstrate the files or registry activities that are associated with the Dropbox cloud service (CS).
3. We collected the unlinked image, which was acquired after unlinking the account from the CS using FTK.
4. We also collected the deleted image which we gained upon deleting some files from the Dropbox CS.
5. Finally, we obtained the uninstalled images when uninstalled the application. Therefore, a keyword investigation scenario conducted for the deleted files.

3.4 OneDrive Forensics

3.4.1. Data Gathering

The assembled data for this scheme combined CSV files obtained from Process Monitor and files from FTK. Figure 3 demonstrates the total amount of filtered files using the Process Monitor for OneDrive cloud service.

3.4.2. Analysis

Our dataset for investigation was derived from the CSV files generated and associated with the examination outcomes of FTK. We focused on analyzing data according to the path results and then filtering them by Excel, such that:

a. Classify the unique paths by:
   - File path.
   - Registry path.

b. To clarify the outcomes, file include the word ‘OneDrive’ were only listed. This step was essential to demonstrate the files or registry activities that are associated with the OneDrive CS.

c. Collect unlinked images which was acquired after unlinking the account from the CS using FTK.

d. Collect the deleted image which we gained upon deleting some files from the OneDrive CS.

e. Finally, acquire the uninstalled images when uninstalled the application. Thus, a keyword investigation senario conducted for the deleted files.

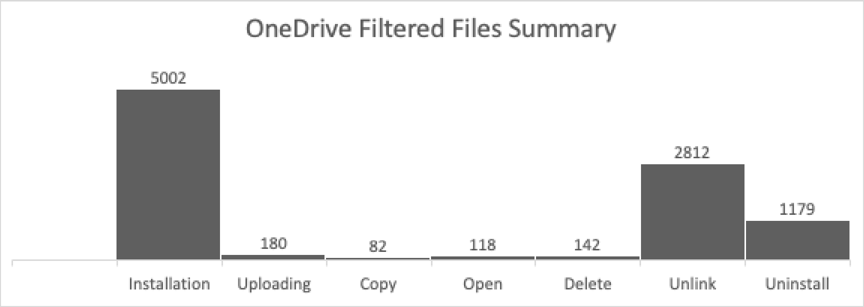

Fig. 3. *OneDrive Filtered Files Summary.*

4. RESULTS

4.1 Results Obtained by Process Monitor

4.1 Results obtained by Process Monitor

4.1.1 Dropbox Results

4.1.1.1 Dropbox client installation scenario

- **3865** artifacts were generated or changed after completing the installation of Dropbox.
- **765** of them were registry paths with the keyword “Dropbox”.
- **60** were file paths included the keyword “Dropbox”.

4.1.1.2 Copying/moving files within Dropbox

- **67** artifacts appeared or modified in the case of copying/moving files in Dropbox.
- **7** of them were registry paths with the word “Dropbox”.
- **35** of them were file paths enclosed the keyword “Dropbox”.

4.1.1.3 Uploading files to Dropbox scenario

- **765** artifacts were generated or changed upon uploading files to Dropbox.
- **4** items were registry paths with the keyword “Dropbox”.
- **36** of them were file paths with the keyword “Dropbox”.

4.1.2 OneDrive Results

4.1.2.1 OneDrive Client Installation scenario

- **3902** artifacts were generated or changed after completing the installation of OneDrive.
- **812** of them were registry paths with the keyword “OneDrive”.
- **76** were file paths that included the keyword “OneDrive”.

4.1.2.2 Copying/ moving files within OneDrive

- **69** artifacts appeared or were modified in the case of copying/moving files in OneDrive.
- **13** of them were registry paths with the word “OneDrive”.
- **37** of them were file paths that enclosed the keyword “OneDrive”.

4.1.2.3 Uploading files to OneDrive scenario

- **817** artifacts were generated or changed upon uploading files to OneDrive.
- **7** items were registry paths with the keyword “OneDrive”.
- **33** of them were file paths with the keyword “OneDrive”.

4.2 Results obtained by Autopsy analysis for E01 image disk

4.2.1 Deleting file scenario

4.2.1.1 Dropbox Results

- There was evidence of test.exe in both pagefile.sys and unallocated space.
- There was no evidence of "Welcome.pdf", but we found a deleted version of "Welcome.pdf" in the

pagefile.sys.

4.2.1.2 OneDrive Results

- In unallocated space and some $Recycle.Bin CSV files, evidence of "dforensics.txt" and "drivetest.png" was traceable, as well as in the AppData.

4.2.2 Unlinking and uninstalling scenario

4.2.2.1 Dropbox Results

- There were two files relevant to "Welcome.pdf" and one file linked to "test.exe" that were left after Dropbox unlinking and uninstallation processes.
- **3703** artifacts were modified when Dropbox in the case of unlinking.
- **1422** artifacts in the case of uninstallation.

4.2.2.2 OneDrive Results

- There were 22 files relevant to "dforensics.txt" and 15 files related to "drivetest" that were left after OneDrive unlinking and uninstallation processes.
- **1170** artifacts were modified when OneDrive in the case of unlinking.
- **4692** artifacts in the case of uninstallation.

5. COMPARATIVE ANALYSIS

Table 1 demonstrates the summary of findings of the cloud clients Dropbox and OneDrive interaction with the system. The table indicates the types of the left behind items that were found after the interaction between the user and the CSPs. The show of results is very close and summarized as follows.

Table 1: Summary of findings for Dropbox and OneDrive cloud client's interaction

	Dropbox	**OneDrive**
Installation	Installation Location	Installation Location
Login	Username, Password, User ID	Username, Timestamp, User ID
Upload	Filename, File-content, File-location, Timestamp	Filename, File-content, File-location, Timestamp
Download	Filename, File-content, File-location, Timestamp	Filename, File-content, File-location, Timestamp
Delete	Filename, File-content, File-location	Filename, File-content, File-location
Move	Filename, File-content, File-location	Filename, File-content, File-location

6. CONCLUSION

The study expressed the challenging use of cloud computing in digital forensics. The investigated problem was to determine whether is it feasible to interpret CSs with conventional methods and if current procedures and tools could operate in cloud forensics. Regarding this, we examined a cloud service provider, developing a case in which we have investigated common SaaS application. After uploading and moving several types of media and files in the cloud, evidence to be found in registry files, logs, and temporary files. Therefore, we have investigated local folders by standard forensic methods to find out the possibility of retrieving possible evidence involving the user and CSP interactions. Some artifacts are dropped behind upon the completion of Dropbox investigation scenarios. Moreover, we noticed that some of the evidences of the files were found in unallocated space. Besides $Recylce.Bin CSV files and pagefile.sys Dropbox remained some trace evidence of the objective files after unlinking and uninstallation processes. Dropbox and OneDrive clients examined. We aimed to prove that it was likely to have forensic copy of the information within the CS by just recovering data or parts of it from local hard drives. The result of the experiment described was unexpected. We have collected compelling evidence of the user-CSP intercommunication by gaining local artifacts without directly reaching to the cloud server. The experiment outcome reveals and illustrate on how essential to examine classical forensic methods are vital for retrieving deleted files and acquire tangible evidence in cloud environment.

7. Future Works

The scope of cybercrimes as well as modern technologies are linked to the global spread of price-affordable smart devices and cloud environments to provide easy access to many forms of data, along with high storage capacities outpacing conventional PCs. In addition, cloud computing becoming widely used and the need for cloud servers' physical accessibility will present difficulty in terms of isolating evidence by common forensic techniques. In cloud forensics, investigation outlining requirements are needed. Today, laws, statutes, and legal practices can range considerably between different service providers. This causes another problem for forensic specialists to operate. As a result, the uniformity of novel cloud forensics procedures will surely denote serious necessity in the field of cloud computing for the near future. Such experimentation exclusively focused on well-known cloud service. Therefore, the service has been almost for several years and will remain useful. In addition, it is necessary to understand when the cloud service accessed by mobile applications disregards traceable artifacts. This condition opens wide background for the following research to discuss if certain data is traceable in the primary state or not. A further potential research is to examine user artifacts interaction between CSPs in order to encounter well defined criminal acts.

8. References

[1] Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 Pandemic. International Journal of Information Engineering & Electronic Business, 13(2).

[2] Rani, D. R., Sultana, S. N., & Sravani, P. L. (2016). Challenges of digital forensics in cloud computing environment. Indian Journal of Science and Technology, 9(17), 1-7.

[3] Galvan, M. (2013). Cloud computing: Incident response and digital forensics (Doctoral dissertation, Utica College).

[4] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[5] Delport, W., & Olivier, M. (2012, January). Isolating instances in cloud forensics. In IFIP International Conference on Digital Forensics (pp. 187-200). Springer, Berlin, Heidelberg.

[6] Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation, 10(1), 34-43.

[7] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). Cloud forensics. In IFIP International Conference on Digital Forensics (pp. 35-46). Springer, Berlin, Heidelberg.

[8] Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. Digital investigation, 13, 38-57.

[9] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90-S98.

[10] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digit. Invest. S87–S95.

[11] Zawoad, S., & Hasan, R. (2015, January). A trustworthy cloud forensics environment. In IFIP International Conference on Digital Forensics (pp. 271-285). Springer, Cham.

[12] Hay, B., & Nance, K. (2008). Forensics examination of volatile system data using virtual introspection. ACM SIGOPS Operating Systems Review, 42(3), 74-82.

[13] Birk, D., & Wegener, C. (2011, May). Technical issues of forensic investigations in cloud computing environments. In 2011 Sixth IEEE international workshop on systematic approaches to digital forensic engineering (pp. 1-10). IEEE.

[14] Wang, W., & Daniels, T. E. (2008). A graph based approach toward network forensics analysis. ACM Transactions on Information and System Security (TISSEC), 12(1), 1-33.

[15] Liu, C., Singhal, A., & Wijesekera, D. (2015, January). A logic-based network forensic model for evidence analysis. In IFIP International Conference on Digital Forensics (pp. 129-145). Springer, Cham.

[16] McClain, F. Dropbox Forensics. 2011. https://articles.forensicfocus.com/2011/07/24/dropboxforensics/ (accessed Mar. 01, 2021).

[17] Quick, D., & Choo, K. K. R. (2013). Dropbox analysis: Data remnants on user machines. Digital Investigation, 10(1), 3-18.

[18] Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. Digital investigation, 9(2), 81-95.

[19] Quick, D., & Choo, K. K. R. (2013). Digital droplets: Microsoft SkyDrive forensic data remnants. Future Generation Computer Systems, 29(6), 1378-1394.