Cloud Storage Forensics: Survey

Sara Abdel Razek[#3], Dr.Heba El-Fiqi[*2], Prof. Dr. Ibrahim Mahmoud[#1]
1, 2, 3, Computer Science Dept., Faculty of Computers and Informatics, Zagazig university, El-Zera Square, Zagazig, Sharqiyah, Egypt

Abstract

Businesses, individuals and government nowadays are looking to use cloud storage services to store their data in favor of having access to them anyplace they are. Increasing usageof cloud storage platforms make the investigation becomemuch more important and difficult.Shortage of knowledge on digital evidence location, privacy issues, and legal boundaries make the digital evidence retrieval from cloud storage services a challenge. Most of the research studies in the literaturefocus on determining the artifactsresult from usingcloud storage applications. Theseapplicationsrunning on various devices and operating systems suggested that artifacts related to install, uninstall, log-in, log-off and others. In this paper, a survey of different researches that investigate cloud storage service is presented. This survey was introduced to give a better understanding of some of the important open key questions of the cloud forensics storagefield to identify promising future research.

Keywords

Digital forensics, Cloud forensics, Cloud storage, Cloud storage forensics, Digital evidence.

1. Introduction

Cloud computing is a technology that grow continuously. Cloud computing can be defined as a group of unlimited virtualized resources which can be easily accessed anytime, anywhere by using internet with no worry about any technical issues[1]. Those resources are (hardware, platform, and services). Customers mustpay for what they use which save their money in comparison with buying local resources. Resources can bereconfiguredto scale them inward and outward dynamically for optimum utilization. The cloud architecture provides three primarycategories of services Infrastructure as a Service, Platform as a Service and Software as a Service[2].We can consider cloud storage services as a form of Infrastructure as a Service which providesstorage space to users for storing their data (files, images, and documents). Cloud storage services provide other servicesas image editing, email-sending, document, playing music and videos. The user has the ability access storage service through software on its personal computer (PC), or installs an application on his mobile device.A survey published by IDC Cloud Services found thatthere are many IT cloud computing concerns as Security 87.5%, Availability 83.3%, Performance 82.9%,High Cost 81%, and Vendor Lock In 80.2%.

Software security problems are increasing and obstructing the growth of Cloud Computing field.Increasing security threats affectscloud computing and makescrimes increase using other types of cloud services. Since there are numerous types of cloud services, there will be variety in the way the criminal investigation is completed in each type of cloud services. Criminal abuse cloud storage service that permits users to store documents and access them overa personal computer ora smartphone[3]. A Criminal could obtain trusted information from a company by abusing a cloud storage service.Cloud storage serviceinvestigation becomes a high priority for forensic experts. A Digital forensic investigatormust be knowledgeable about the different providers of cloud storage to provide efficient investigations.In the following literature review, we explore the procedures and approaches used by different research studies to investigate various cloud storage service on different devices. In Section 2 we present digital forensics categories and various digital forensics tools. In Section 3 we discuss cloud forensics and some of the challenges in cloud forensics area. Section 4 we introduce a review of Strategies and Techniques which are used in digital forensic investigation in cloud computing storage service. We end with a discussion in section 5 and conclusion remarks and future work in section 6. The appendix summaries our survey findings of cloud storage forensics researches, categorized by research methodology.

2. Digital forensics investigation and Forensics tools

The American Heritage Dictionary defines forensic as “relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law [Hou00].”Considering the digital evidence, technology is always needed to process the digital data. The main difference between a forensic and a non-forensic investigation of digital data is that the evidence in forensic investigation can be used in a court of law. The preceding section discussed the digital forensics concept, the Digital Forensics categories and the advantage of using forensics tool through some research papers.

2.1 Digital Forensics

Digital forensics is a branch of forensic science including the retrieval and investigation of artifacts found in digital device often conducted as aresponse to computer crime. Digital forensics has become an important tool in identifying computer-assisted crime. Digital Forensic Research

Workshopin 2001 defines digital forensics as the utilization of scientific methods for preserving, collecting, validating, identifying, analyzing, interpreting and documenting of digital evidence obtained from digital sources for the purpose of facilitating or furthering the reconstruction discovered to be criminal or helping to foresee unauthorized actions shown to be disruptive to planned operations. NIST Cloud Computing Reference Architecture definesdigital forensics asthe application of science for identifying, collecting, examining,and analyzing of data while preserving the information integrity and maintaining the data custody.The Digital Forensics categories are applicable to the cloudand otherssuch as computer forensics, network forensics, database forensics and mobile forensics. Differences between these categories are discusses briefly in the following subsections.

A. Computer Forensics

Computer forensics was developedbecause of the personal computer rapidevolution. Criminals have the ability to use a user personal computer for criminal means. The usage of computer forensics grew from the mid of1990s to 2000s. This necessitate computer forensic investigators to developtheir own custom tools that are able to process what they specifically needed during analysis of evidencesrather than copying hard drives bit for bit then conducting the required analysis.Computer forensics is not just limited to white collar crime, child pornography, and malicious code investigations. Computer forensics is a vital component of the war on terrorism, and homeland security. A survey[4] was published to provide a more up-to-date prospective on what computer forensics researchers and practitioners felt were the top five issues facing the discipline.

B. Network Forensics

Cloud computing is based on broad network access and follows the main phases of network forensics. Using infrastructure as a service instance in distributing a malware, it is difficult to gatherthe routing information and network log even if they are important for forensic data collection. Network forensics is defined in Palmer (2001) as ‘‘use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.’’

Network forensics used in analyzing network traffic and logs for events that have happened in the past[5].Capturing network activity using forensic analysis is simple in theory, but in practice it is a trivial.SrinivasMukkamala et. al. [6]focus on network forensics and offline intrusion analysis. The research also focuses on related issue of finding important input features for computer forensics and intrusion detection. Emmanuel S. Pilli et. al.[7]gave an overview on network forensics covering tools, process models and framework implementations.

C. Database Forensics

We can define database forensics as the application of computer investigation and examination techniques to find the evidences suitable for presentation in court of law. Using database forensics, we can distinguish datapre and post transaction, recover the previous deleted data rows, prove data security breach and others. Database Forensics is a significantarea that has received research attention. Martin S. Olivier[8] considers the differences between databases and file systems then transfers file system forensics concepts to database forensics concepts.

D. Mobile Forensics

Mobile devices can be considered asource of evidence in wide-ranging crimes, such as fraud, and data theft. New acquisition methods have developed to give forensic practitioners access to additional information on mobile devices, including deleted data. Eoghan Casey et. al. [9] covered various methods to acquire and analyzed data on Windows Mobile devices using both commercial and open source tools. Since it became difficult for a professional investigator to select theproper forensics tools for seizing internal data from mobile devices, Maynard Yates[10] gives a complete perspective of every popular digital forensic tool and provide an inside view for investigators to select their free sources or commercial tools.

E. Cloud Forensics

Cloud forensics is a standout amongst the most challenge fields in digital forensics nowadays. Cloud forensics is digital forensics applied on cloud environment to gather information for investigation. Cloud forensics consists of more than one dimension which is Technical, Organizational and Legal. Ruan et al. [11] present the survey results that was circulated among digital specialist globally on cloud forensics and critical criteria for cloud forensic capability to well understand the most important fundamental issues ascloud forensics definition, cloud forensics scope, cloud forensics challenges and opportunities.

2.2 Digital Forensics tools

An investigator can view the directories and files of a suspected system by using either forensic software or by using the operating system of an analysis system. Both methods are possible to view evidence in allocated files, but only the specialized forensic software enables him to obtain unallocated files easily. The rapid advance of cloud services requires the development of better forensic tools tokeep pace[12].Brian Carrier [13] described the purpose and objectives of digital forensic analysis tools using the theory of abstraction layers and examined the nature of tools in digital forensics and proposes definitions and requirements.RFM Roman et al.[14]focusedin analyzing the computer forensicstools throughgathering bibliographic data, and assessment of indicators distinguishing devices that present all the more adequately in the field of Computer Forensics.NDW Cahyani et al.[15]introducean overview of the current capability of mobile forensic tools and the challenges in successfully extracting evidence from Windows phone platform. J Dykstra [16]aim todesign, implement, and evaluatethree new forensic tools for the OpenStack cloud platform.Matthew Geiger [17] focused on evaluating commercial counter-forensic tools and review the performance of six tools and highlight operational shortcomings that could permit the recovery of important evidentiary data.

3. Cloud storage forensics analysis

3.1 Cloud storage service

Cloud storage offersstorage with scalable and elastic capabilities that can be delivered as a service using internet technologies[18].We can consider cloud storage services as Infrastructure as a service which provide users with storage space and additional services such as document and image editing, the capabilityof playing music and videos, and email-sending capacity. Cloud storage service can be accessed in various ways such as using software application or using a web browser in accessingcloud storage service on a personal computer, or install an software application on a mobile device. Examples of Cloud storage hosting providers are (Google Drive, Microsoft One Drive, Adrive, SugarSync, Dropbox, etc…).Most of Cloud storage hosting providers offer limited cloud storage space and you can upgrade limited space with additional fees. The main benefits of a public storage service are: availability where customer can access data from any machine and at all times; reliability where data of the customer is backed up; efficient retrieval and data sharing where customers can share their data with trusted parties[19]. An extensive variety of users and applications are using cloud storage service from cloud providers to accomplish their tasks. They put their trust in the cloud provider's security of its access controlmechanisms.As with most new technologies cloud storage services are exposed to attack and exploitation by criminals,so we have to forensically analysis these storage platforms.The 2011 online data breach involves the abuseof Amazon servers by cybercriminals to cripple Sony PlayStation Network. A number of papers that discuss the use of cloud storage services by criminals and forensic examinations are published.

3.2 Cloud Forensics

The evolution of cloud computing has introduced a new term cloud forensics. NIST defines cloud forensics as the application of digital forensic science in cloud environments. In Technical view, it consists of a hybrid forensic approach towards digital evidence generation. Organizationally it involves interactions between cloud actors for facilitating both inner and outer investigations. Legally it often implies multijurisdictional and multi-tenant situations (NIST, 2014a). According the survey results [11] cloud forensics cannot be considered to be internet forensics or classical computer forensics, nor a brand new area. It is rather a combination of traditional forensic techniques and their applications in cloud computing environment.NIST have categorized nine groups of Cloud Forensics major challenges which are[20]:

1. Architecture such as diversity, complexity, provenance, multi-tenancy and data segregation
2. Data collection such as data integrity, data recovery, data location and imaging.
3. Analysis such as correlation, reconstruction, time synchronization, logs, metadata and timelines.
4. Anti-forensics such as obfuscation, data hiding and malware.
5. Incident first responders such asthe trustworthiness of cloud providers, response time, reconstruction.
6. Role management (e.g., data owners, identity management, users and access control.
7. Legal such as jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy and ethics.
8. Standards (e.g., standard operating procedures, interoperability, testing and validation.
9. Lack of Training (e.g., forensic investigators, cloud providers, qualification and certification.

Cloud Forensics involves post attack investigation for knowing the attack source and collect evidence[21].We can extract the evidence from three sources which are cloud service providers' management server, network layer and client system. Data acquisition from the client and network layer is easier than gathering evidence from cloud service provider because of privacy concerns[22].According to the definition of digital forensic by McKemmish (1999)[23] , forensic computing can be defined as the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally

acceptable. It encompasses four key elements.The first element is digital evidence identification. It is important to know what evidence is present, where it is stored and how it is stored to determine which processes are to be employed to facilitate its recovery. Forensic computing can spread out to cover any electronic device that have the capability of storing information.The forensic examiner must have the ability to identify the format and the type of information stored in the device to determine the appropriate technology to be used. The second element is the digital evidence preservation. Digital forensic investigation is conducted through analysis of forensic copy of data, rather than altering or interacting with the original source. The third element is digital evidence analysis by correlating and assimilating material to produce reasoned conclusions. This is the main element in forensics computing. Digital evidence requires processing before being read by people. The last element is digital evidence presentation, which involves the actual presentation in a court of law.

Cloud forensic are applied to the various types of cloud services as cloud storage service.Cloud storage services are vulnerable to exploitation and attack by criminals, a criminal could leak confidential information from a company by abusing a cloud storage service that allows users to store documents, images and others. It is not impossible to investigate criminal cases that involve cloud storage service, because traces of using the service are left in a user's device. Forensic examiners must know the different types of cloud-based storage systems available and what artifacts each may leave behind, in order not to miss critical information during an investigation. A number of forensic researchers have examined many popular cloud apps in recent years to identify a range of artifactsarising from using cloud storage application. Most of researches focus on gathering evidence from devices either personal computer and/or mobile device with various operating systems to find artifacts left by cloud storage applications that suggests their use even after the deletion of the applications.Other research efforts include evaluation of the effectiveness of commercial forensic tools in acquiring evidence remotely fromvarious cloud storage provider or determining whether the act of downloading data from the client and web applications of popular cloud services (i.e., Dropbox, Google Drive, and Microsoft SkyDrive) affects the integrity of the data collection process or Providing frameworks, guidelines, and methodologies with the aim of providing a systematic approach for forensic collection of cloud artifacts from servers and/or client devices.

3.3 Challenges of cloud forensics

In this section, we discuss some of the challenges in cloud forensics which must be considered to recover.Josiah Dykstra et. al[24] present cloud crimes through two hypothetical case studies; compromised cloud- based website and child pornography that are hosted in the cloud. The paper highlighted the weakness of current forensic practices and describes cloud forensics challenges, including forensic acquisition, evidence preservation and chain of custody, and open problems.Stephen Mason et. al[25] has explained the effect that 'cloud' computing might have on evidence in digital format in criminal proceedings in the jurisdiction of England & Wales. The problems that cloud computing might bring to criminal investigations are discussed as copies of data, seizing evidence, need of storage device, and law enforcement challenges.Stephen Biggs et. al[26] highlight where the Impact of Cloud Computing will diversely affect digital forensic investigations. These impacts are service level agreements which must be robust, attackson cloud and CIA (confidentiality, integrity, availability) model of information security.

4. Current practices: Strategies and Techniques

In this section,we introduce a review of Strategies and Techniques which are used in digital forensic investigation in cloud computing storage service.Researchers have analyzed forensic investigation of cloud computing storage services through storage devices as Windows system, Mac system, iPhone, and Android smartphone.Important factors that affect the investigation are log files of web browsers, artifacts of client applications in PC, artifacts in smartphones, and physical memory.Some researchers have discussed the challenges of forensic investigation in cloud computing environment with solution in the form of several phases of digital forensics in cloud environment. The following is a summarized discussion of the prior work.

4.1 Digital Investigative Process (DIP) model proposed by the first Digital Forensic Research Conference Workshop (DFRWS)

Ben Martini et. al [27]have focused on client and server artifacts that found in open source cloud Storage as a service (StaaS) application ownCloud. Investigation the devices of the client that demonstrated in many cases we can found critical data which links to a specificownCloud instance. This provides a forensic path to the ownCloud server instance even when evidential data on the client may be removed securely. Papershows discussion from both client and server perspectives cloud StaaS forensics but not all artefacts covered on both on client side and server side.

SathishkumarEaswaramoorthy et. al. [28] identify the client evidence data on"window7" and provide a clear idea about type of evidences are exist in machine for forensics practitioner using two

popular public cloud service providers (Microsoft One Drive and Amazon cloud drive).Possible evidence determined include file timestamps, file hashes, client software log files, memory captures, link files and other evidences using forensic analysis which is the procedure of acquisition, preservation and examination of evidence data from computer systems, networks, and storage devices for judicial purposes, such as criminal investigations or civil cases.

4.2 Cloud forensics framework of Martini and Choo

Yee-Yang Teing et. al. [29] aim to collect data remnants and identify terrestrial artefacts that remain after using cooperative cloud storage services such as Symform using both mobile and personal computers deviceswithdifferent popular operating systems as Win 8.1, Mac OS X Mavericks, Ubuntu, iOS, and Android KitKat.The research suggested that there is currently no method known outside the client application or CSP that allows reconstruction of the synchronized files from the file fragments.

4.3 Digital Forensic Analysis Cycle Model

Darren Quick et. al. [30] aim to clarify terrestrial artefacts that remain onthe machine of a client (ex: computer hard drive and iPhone device) after a user accesses Microsoft SkyDrive. Using digital forensic analysis cycle commence (scope), prepare, identify, collect, Preserve, Analysis and Presentation". It was discovered that an investigator can distinguish SkyDrive account use by attempting keyword searches, hash comparison, and inspect common file locations in Windows 7 systems to locate relevant information.

Darren Quick et. al. [31] focus on discovering the remnants left on client devices (computer and iPhone) after a user accesses Google Drive storage service,and examining the benefits of using a suggested framework to help in investigation when undertaking forensic analysis of a cloud environment.It was discovered that an practitioner can identify the usage of Google Drive account by undertaking keyword searches and check common file locations to locate relevantinformation.

4.4 McKemmish model

S. Mehreen et. al. [32] aims at finding the data remains fromDropbox cloud storage on Win 8 platform. The procedures for computer forensics consists of four steps identify, preserve, analyze and present. This paper concludes that the artifacts found on local machines carry critical information in registry and local folders in different locations and identified the data locations of data to determine user details and cloud storage information relating to use of Dropbox.

Darren Quick et. al. [33]work on collecting artefacts from a cloud storage account of three cloud storage service providers Dropbox, Google Drive, and Microsoft SkyDrive through a browser client and furthermore downloading files using client software and then comparing with the original files and undertake analysis of the resulting data. Identification, Preservation, Analysis and Presentation are four steps used in Cloud Storage Data Collection strategy. Thereforecontents of files did not change during the process of uploading, storage, and downloading files from cloud storage accounts. This research will help in criminal investigations and civil litigation matters.

Darren Quick et. al. [34] adopt the methodology proposed by McKemmish (1999) consisting of the coming steps; identify, preserve, analyze, and present for determining the data artefacts on a Win 7 personal computer and iPhone 3G when a user undertakes different methods for storing, uploading, and accessing data in the cloud. The research authors have identified the data and files locationsas directory listings, prefetch files, link files, thumbnails registry, browser history, and memory captures used to obtain user details and cloud storage information.

4.5 Configuration, Data Collection and Result

Kurt Oestreicher[35] has focused on determining the directories of iCloud-synched files in Mac OS to know if file hash values match those of the original files or not. The challenges are given in form of three phases; these phases are Initial configuration, Data Collection and Result. This research limitation is that it focused on inspection of files transferred from a Mac OS X 10.9 machine to the iCloud server.

4.6Using different programs and tools

Methodology followed is to use different tools and software programs to perform the research and to collect the data. Rakesh Malik et. al. [36]use different tools and software programs tocollect evidence from different devices to findartifacts left by cloud storage applications that suggest their use even after the removal of the applications. The research showed that we can find plenty of evidence that related to the usage of cloud storage client application and also highlighted the main paths, directoriesand files on a client device with different types of operating systems Ubuntu 14.04, Android OS and Win 8.1. Some tools that used to automatically find evidence were SQLite Browser, Process Monitor, Process Explorer, Wireshark, RegScanner,TheSleuth Kit and others. Programs used to find evidence in Ubuntu also varies. Locations of evidence and file types may vary in "UNIX/Linux" operating system (Ubuntu 14.04)

because of the different features of the Windows operating systems and the UNIX/Linux OS.

Rakesh Malik et. al.[37]Highlighted the main paths, directories and files on a client device with an operating system "Ubuntu 14.04", and more generally, "UNIX/Linux" operating systems. Methodology is to use tools and software programs such as VMware Workstation 10 for creating a virtual machine of "Ubuntu 14.04" ("Trusty Tahr").Another tools used such as LiME, TheSleuthKit,istat, Foremostand and SQLite Browser.Some Command line executed on terminal such as find, grep, lsof (list open file) and command. Unfortunately, the number of tools used to analyze dynamically a process, such as Process Monitor doesn't available for UNIX/Linux. As a conclusion, it was still possible to find evidence in the hidden directories or hidden files created by the application, as in database or log files, inside web browser files, in the memory, and in both allocated and unallocatedspace.

Rakesh Malik et. al.[38]Examined the remaining artifacts of Cloud storage services (Dropbox, ownCloud) on "Windows 8" operating system. Both a static analysis and a dynamic analysis are used to collect data. A number of applications were used as Process Monitor, Process Explorer, SQLite Browser, SQLite Browser and others. The research result stated that a large number of files are affected during the application installation, and a large number of files are left behind, once the uninstallation process is completed.

Mohammad Shariatia et. al. [39] focus on determining the types and nature of data that can be recovered from "Windows 8", "Mac OS X 10.9", "Android 4" and "iOS 7" devices using "SugarSync" (a popular cloud storage service). The Paper aimsat determining and documenting digital artifacts when the user had used SugarSync to upload or download file or folder. Some of the tools used in this research are Regshot, Process Monitor and Nirsoft browser. This research proved that SugarSync credentials, method of access, filenames and associated metadata can be retrieved when SugarSync is used as cloud storage service.

4.7Designing new acquisition tool

Some of the researches introduce new approach of designing and implementing new acquisition tool to acquire evidence.VassilRoussev et. al.[40] present an acquisition tool, "kumodd" which can obtain evidence from four major cloud drive providers (Google Drive, Microsoft OneDrive, Dropbox, and Box). The prototype of acquisition tool kumodd is written in Python and offers both a command-line and web-based user interfaces.

4.8Different procedures and methodologies

In this section the researchers introduce different procedures and methodologies to investigate cloud storage services. Hyunji Chung et. al. [3] introduce new procedure for investigating and exploring the artifacts of cloud storage services for the Windows, Mac, iOS, and Android operating systems.This paper discussescritical factors that must be taken in consideration in a forensic investigation and deals with the created traceswhen a cloud storage service is used with a Mac and windows system. Artifacts that are left when a cloud storage service is used with two representative smartphone operating systems, namely iOS and Android are discussed. The research result states that the confidential file was found using Dropbox and by analyzing the prime suspect's PC and smart-phone together, more precise investigation was possible.This paper has presentedunknown method for forensic analysis of cloud storage services for the Mac, iOS, Windows, and Android operating systems which help in investigating of cloud storage services.

George M. Kiruthu[41]aim to obtainthe digital artifacts in a shared folder in the cloud-based service, Dropbox, by developing an admissible method of digital evidence collection. The goal of the research was to answer a question "What is an admissible method for extracting digital evidence from a shared Dropbox folder in a multi-platform cloud environment?" .The research methodology used was broken into three steps. First step include setting the categories of forensic requirements. Second step is to implement the cloud storage infrastructure involving identification and collection of digital evidence artifacts of Win 2008 server, Win7, Ubuntu virtual images, and a MacBook hard drive image.Third one is to analyses data in order to determine if the research goals were verifiable or not.The result of experiment said that it was possible to retrieve or extract significantdigital information from a cloud-shared Dropbox folder.

Shujian Yang [42] aim to collect as much valuable evidence as possible in a Google Drive account while maintaining integrity of evidence. There are two research questions to be answered "What types of evidence in Google Drive can be found via the API approach?" and "How was the integrity of evidence maintained during the acquisition via the API approach?". The research mentioned the Studies of Google Drive Forensics as literature review. The author focused on personal used cloud storage services becauseit is difficult to develop a forensic tool to cover all cloud storage services even when considering a single cloud storage service provider, problems still exist. This research can help digital forensic examiners choose the most convenient tool to perform their tasks.

Yee-Yang Teing et. al. [43] aim to find data remnants from using the BitTorrent Sync applications (version 2.x) using computer devices running Windows, Mac OS, Ubuntu, iOS, and mobile device running Android after doing variousactivities such as installation, uninstallation, log-in, log-off. Research methodology involves three main steps.The initial step was setting up the test environments for the client applications for a MacBook Pro running Mac OS X Mavericks and iPhone 4 running iOS and an HTC One X running Android KitKat. The second step was setting up a list of activities to simulate various real world scenarios of using the applications. The third step was to prepare the forensic workstation with a number of tools which used in forensic investigations. The last step was to test data matching the terms 'Bittorentsync','btsync' and 'Enron3111' in the forensic images.The contribution of this research is using the newer client applications (version 2.x) on a wide range of computer and mobile devices .The research also detailed the artifacts from the data files as well as volatile evidence sources.

Ben Blakeley et. al. [44] aim to find remaining artifacts by investigating of hubiC as one of popular cloud platforms running on Win8.1 after different usages such as upload, download, installation, and uninstallation. This paper aims toanswer following questions "What data can be recovered on the hard drive or physical memory of Windows 8.1 machine after using the hubiC cloud storage service?" and "What data is transmitted in the network traffic during communication during upload and download?". Results of investigating the Access VM, Upload VM, Download/Open VM, Delete VM, Install Desktop VM, Upload Desktop VM, Uninstall Desktop VM, Download Desktop VM and Delete Desktop VM, including memory forensics and temporary and log files analysis are presented.

Jason S. Hale One [45]aim to find the artifacts of using Amazon Cloud Drive.The paper describes the methods of forensic analysis of cloud storage service in three points. First is accessing the Cloud Drive with the user's credentials to determine what files are stored on the Cloud Drive. Second is to extract the browser cache files from the local machine. Last is to extract the ADriveNativeClientService.log file from the local machine and view the information files related toAmazon Cloud Drive usage.

5. Discussion

Previous studies have noted the importance of forensics analysis for cloud storage services. Different methods of forensic analysis are used to find data remnants after using cloud storage applications using mobile or computer devices running various operating systems. Surprisingly, most of the researchers were found to identify the evidence data on a client device using Window7, Windows8.1, android, iOS and Mac operating system. Dropbox, Google Drive and SkyDrive are most commonly used cloud storage application, while iCloud, SugarSync, Microsoft one drive and hubiC are slightly used. More research is needed to cover most recent operating systems such as windows10 and other Linux distributions. One key strength discussed in study [40] is introducing a new tool kumodd to perform cloud drive acquisition from four major providers. Another key strength found when the researchers in [33] verify their finding through conducting an analysis using commercial forensic tools as X-Ways, AccessData Forensic Toolkit. Expansion within most of the researchers also remains to cover all the artifacts on both sides on client and server. Mohammad Shariati and other researchers [39]work on SugarSync (a popular cloud storage service) that haven't discussed on wide range but the tools used (Digital Detective Net Analysis) hadn't the ability to run on virtual environments. This issue can be discussed later in other researches. The work introduced by Ben Martini et. al. [27] was the first to provide a complete discussion on cloud StaaS forensics from both client side and server side but not all the artifacts was covered. Unknown method of forensic analysis was discussed by Hyunji Chung et. al.[3]. One key advantage of this paper is proposing a model of process for forensic investigation of cloud storage services of different operating system. The weakness that this paper doesn't focus on physical memory. We found that most of the studies focus on finding data remnants on windows7. But not all artifacts can be covered on both client side and server side.The only paper [27]that provides a holistic discussion on cloud StaaS forensics from both client and server side. This paper found digital forensic artifacts of ownCloud application on centos operating system. Centos operating system wasn't discussed a lot in other researches.

Yee-Yang Teing et. al. [43] focused on the newer client applications BitTorrent (version 2.x) on a wider range of computer and mobile devices running several operating systems. This researchdidn't include incorporating the collection and investigation of data artefacts from different IoT middleware. Case study was prepared in [30] and [33]to illustrate the relevance of the research. Providing case study outlines where the information previously identified and also assist in an investigation.Rakesh Malik et. al. [36] use different tools and software programs to find a plenty of evidence that related to using cloud storage client application. A lack of analysis tools for Android OS didn't let us perform a dynamic search to collect the

useful data artefacts.Future work remains in several areas as identifying evidence data on more cloud storage applications and covering most recent operating systems.

6. Conclusion Remarks and Future work

Cloud storage service will remain a popular medium used in transferring files for the foreseeable future. Digital forensic examiners will need to know about the different cloud storage providers so that they can conduct thorough, accurate, and efficient investigations. This survey paper provides the most challenging issues and the most valuable research directions for cloud storage forensic. With the increase in research and practical use towards cloud storage forensics, we survey the forensic challenges in cloud storage services and analyze their most recent solutions and limitations.Research challenges suggested in the literature and also by identifying the gaps in papers surveyed are listed. As the development of cloud forensics is still at an early stage, we hope our work will provide a better understanding of the challenges of cloud storage forensics. This survey was created to gain a better understanding on cloud storage forensics field before further research and development. We would like to examine one of the most popular cloud storage services on a newer version of operating system. Extending this survey to other categories of forensics techniques such as cloud malware forensics, mobile device cloud applications forensics, social network platforms investigation of cloud systems, and cyber-crime and cyberwar investigation techniques in cloud environments would expand this to a comprehensive body of knowledge.

References

[1] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.ISO 690

[2] Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to cloud computing. Cloud computing: Principles and paradigms, 1-41.

[3] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digit. Investig.*, vol. 9, no. 2, pp. 81–95, 2012.

[4] M. K. Rogers and K. Seigfried, "The future of computer forensics : a needs analysis survey," pp. 12–16, 2004.

[5] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digit. Investig.*, vol. 13, pp. 38–57, 2015.

[6] S. Mukkamala and A. H. Sung, "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques," vol. 1, no. 4, pp. 1–17, 2003.

[7] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks : Survey and research challenges," *Digit. Investig.*, vol. 7, no. 1–2, pp. 14–27, 2010.

[8] M. S. Olivier, "On metadata context in Database Forensics," *Digit. Investig.*, vol. 5, no. 3–4, pp. 115–123, 2009.

[9] E. Casey, M. Bann, and J. Doyle, "Introduction to Windows Mobile Forensics," *Digit. Investig.*, vol. 6, no. 3–4, pp. 136–146, 2010.

[10] Yates, I. I. (2010, October). Practical investigations of digital forensics tools for mobile devices. In 2010 information security curriculum development conference (pp. 156-162). ACM.

[11] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," Digit. Investig., vol. 10, no. 1, pp. 34–43, 2013.

[12] NIST Cloud Computing Forensic Science Working Group. (2014). NIST Cloud Computing Forensic Science Challenges.

[13] B. Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," vol. 1, no. 4, pp. 1–12, 2003.

[14] R. Fernando *et al.*, "Digital Forensics Tools," vol. 11, no. 19, pp. 9754–9762, 2016.

[15] L. Adhianto *et al.*, "HPCTOOLKIT: Tools for performance analysis of optimized parallel programs," *Concurr. Comput. Pract. Exp.*, vol. 22, no. 6, pp. 685–701, 2010.

[16] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Digit. Investig.*, vol. 10, no. SUPPL., pp. S87–S95, 2013.

[17] M. Geiger, "Evaluating Commercial Counter-Forensic Tools," pp. 1–12, 2005.

[18] Harnik, D., Pinkas, B., & Shulman-Peleg, A. (2010). Side channels in cloud services: Deduplication in cloud storage. IEEE Security & Privacy, 8(6), 40-47..

[19] D. Hutchison and J. C. Mitchell, Lecture Notes in Computer Science. .

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

[21] A. K. Mishra, P. Matta, E. S. Pilli, and R. C. Joshi, "Cloud Forensics : State-of-the-Art and Research Challenges," 2012.

[22] Birk, D., & Wegener, C. (2011, May). Technical issues of forensic investigations in cloud computing environments. In Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on (pp. 1-10). IEEE.

[23] McKemmish, R. (1999). What is forensic computing?. Canberra: Australian Institute of Criminology.

[24] J. Dykstra and A. T. Sherman, "UNDERSTANDING ISSUES IN CLOUD FORENSICS : TWO HYPOTHETICAL CASE STUDIES," no. 45, p. 2011, 2011.

[25] S. Mason and E. George, "Digital evidence and ' cloud ' computing," *Comput. Law Secur. Rev.*, vol. 27, no. 5, pp. 524–528, 2011.

[26] S. Biggs and S. Vidalis, "Cloud Computing : The Impact on Digital Forensic Investigations," 2009.

[27] B. Martini and K. K. R. Choo, "Cloud storage forensics: OwnCloud as a case study," *Digit. Investig.*, vol. 10, no. 4, pp. 287–299, 2013.

[28] S. Easwaramoorthy, S. Thamburasa, G. Samy, S. B. Bhushan, and K. Aravind, "Digital forensic evidence collection of cloud storage data for investigation," *2016 Int. Conf. Recent Trends Inf. Technol. ICRTIT 2016*, 2016.

[29] Y. Teing, B. Sc, A. Dehghantanha, D. Ph, K. R. Choo, and D. Ph, "DIGITAL & MULTIMEDIA SCIENCES Forensic Investigation of Cooperative Storage Cloud Service : Symform as a Case Study," no. May, 2016.

[30] D. Quick and K. K. R. Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," *Futur. Gener. Comput. Syst.*, vol. 29, no. 6, pp. 1378–1394, 2013.

[31] D. Quick and K. K. R. Choo, "Google drive: Forensic analysis of data remnants," *J. Netw. Comput. Appl.*, vol. 40, no. 1, pp. 179–193, 2014.

[32] S. Mehreen and B. Aslam, "Windows 8 cloud storage analysis: Dropbox forensics," *Proc. 2015 12th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2015*, pp. 312–317, 2015.

[33] D. Quick and K. K. R. Choo, "Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?," *Digit. Investig.*, vol. 10, no. 3, pp. 266–277, 2013.

[34] D. Quick and K. K. R. Choo, "Dropbox analysis: Data remnants on user machines," *Digit. Investig.*, vol. 10, no. 1, pp. 3–18, 2013.

[35] K. Oestreicher, "A forensically robust method for

acquisition of iCloud data," *Digit. Investig.*, vol. 11, no. SUPPL. 2, pp. S106–S113, 2014.
[36] R. Malik, N. Shashidhar, and L. Chen, "Cloud Storage Client Application Analysis," *Lei Chen Int. J. Secur.*, no. 91, pp. 2015–1, 2015.
[37] R. Malik, N. Shashidhar, and L. Chen, "Cloud Storage Client Application Analysis on UNIX/Linux," *Lei Chen Int. J. Secur.*, no. 91, pp. 2015–1.
[38] R. Malik, N. Shashidhar, and L. Chen, "Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform," p. 15.
[39] M. Shariati, A. Dehghantanha, and K. Raymond, "Australian Journal of Forensic Sciences SugarSync forensic analysis," no. April 2015, pp. 37–41.
[40] V. Roussev, A. Barreto, and I. Ahmed, "API-based forensic acquisition of cloud drives," *IFIP Adv. Inf. Commun. Technol.*, vol. 484, pp. 213–235, 2016.
[41] Kiruthu, G. M. (2012). Digital forensic investigation of a Dropbox cloud-hosted shared folder (Doctoral dissertation, Purdue University).
[42] "Running head : GOOGLE DRIVE FORENSIC ANALYSIS VIA API Google Drive Forensic Analysis via Application Programming Interface A Thesis Presented to the Faculty of Jackson College of Graduate Studies University of Central Oklahoma In Partial Fulfillment of the Requirements of the Degree of MASTER OF SCIENCE in FORENSIC SCIENCE by Shujian Yang," 2015.
[43] Y. Teing, A. Dehghantanha, and K. R. Choo, "Forensic investigation of P2P cloud storage services and backbone for IoT networks : BitTorrent Sync as a case study," *Comput. Electr. Eng.*, vol. 0, pp. 1–14, 2016.
[44] B. Blakeley, C. Cooney, A. Dehghantanha, and R. Aspin, "Cloud Storage Forensic : hubiC as a Case-Study," vol. 1, 2015.
[45] J. S. Hale, "Amazon Cloud Drive forensic analysis," *Digit. Investig.*, vol. 10, no. 3, pp. 259–265, 2013.

7.Appendix A. Existing cloud storage forensic researches

Paper Name	Author	Year	Cloud Service	Platform	Tool or Strategy	Notes	
						Advantage	Limitations
DIGITAL FORENSIC INVESTIGATION OF A DROPBOX CLOUD-HOSTED SHARED FOLDER	George M. Kiruthu	2012	Dropbox	Windows User2008 Server Windows 7 MacBook Ubuntu	1- Establishing the categories of forensic requirements. 2- Implementing cloud storage infrastructure and necessary procedures for evidence acquisition. 3- Analyzing the evidentiary data to know if the goals were verifiable.	Valuable artifacts obtained from the Win2008, Win7, Mac OS, Ubuntu images, and the Dropbox web.	This research is limited to forensic acquisition of data objects and their artifacts, Only a limited number of users, software, and equipment are analyzed.
Google Drive Forensic Analysis via Application Programming Interface	Shujian Yang	2015	Google Drive	Windows 7	1- Authentication. 2- Data Integrity. 3- Data Acquisition. 4- Output.	This research utilized Google Drive API as the tool to collect evidence from Google Drive.	It is extremely difficult development of universal forensic tool to cover all cloud storage services. This research focuses on personal use of cloud storage services.
Cloud Storage Client Application Analysis	Rakesh Malik, NarasimhaShashidhar& Lei Chen	2015	SkyDrive Google Drive Dropbox	Ubuntu 14.04 Android Windows 8.1	Methodology is to use tools and software programs as LiME, TheSleuth Kit, istat, Foremostand and SQLite Browser.	Finding a plenty of evidence that related to using cloud storage client application, and evidence that relates to the activity of the user.	A lack of analysis tools for "Android OS" didn't let us perform a dynamic search to collect the useful data artefacts.
Dropbox analysis: Data remnants on user machines	Darren Quick*, Kim Kwang Raymond Choo	2013	Dropbox	Windows 7 Apple iPhone 3G	In this research, they adopt the methodology proposed by McKemmish (1999) consisting of the following 1.steps; 2.identify, 3.preserve, 4.analyze, and 5.present.	The scope of the research is to find the data remnants on "Windows 7" for using Dropbox.	Research was limited by not having the capability to jailbreak the iPhone.
Paper Name	**Author**	**Year**		**Platform**	**Tool or**	**Notes**	

			Cloud Service		Strategy	Advantage	Limitations
Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study	Yee-Yang Teing, Ali Dehghantah, Kim Kwang Raymond Choo , Laurence T Yang	2016	BitTorrent Sync	Windows 8.1 Mac OS– Mavericks 10.9.5 Ubuntu 14.04 Android – Kitkat version4.4.4	1- Setup the testing environments for the client, which consisted of two (2) VMWare Workstations (VMs), repre0senting (host and guest workstations. 2- They conducted a predefined number of activities to simulate various real cases of using the applications.	They focused on the newer client applications BitTorrent (version 2.x) on a wider range of computer and mobile devices running several operating systems.	The research not includes incorporating the collection and investigation of data artefacts from different IoT middleware.
Cloud storage forensics: ownCloud as a case study	Ben Martini*, Kim-Kwang Raymond Choo	2013	ownCloud	Windows 7 Server Centos 6.3	1- Identify evidence Source and preserve. 2- Collection. 3- Examine and Analysis. 4- Report and present.	First paper that provides a holistic discussion on cloud StaaS forensics from both (client and server) sides.	Not all artefacts covered on both sides of (client and server)
Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study	Yee-Yang Teing, Ali Dehghantana, Kim-Kwang Raymond Choo, TooskaDargahi and Mauro Conti.	2016	Symform	Windows8 Mac OS Mavericks iOS 7.1.2 Ubuntu 14.04 Android Kitkat version 4.4.4	1- Identify evidence Source and preserve. 2- Collection. 3- Examine and Analysis. 4- Report and present.	This paper makes us understand the types of terrestrial artifacts that stay from utilizing cooperative storage cloud on client devices.	Artefacts not covered on server side.
Digital Forensic Evidence Collection of Cloud Storage Data Investigation	SathishkumarEaswaramoorty, SankarThamburasa, Guru Samy, S.BharathBhushan, KarrothuAravind	2016	Microsoft one drive Amazon cloud drive	Windows 7	1- Identify evidence Source and preserve. 2- Collection. 3- Examine and Analysis. 4- Report and present.	The proposed framework will help to guide the examiners in a digital forensic evidence collection process from starting to completion.	This research applied only on one release of windows operating system.
Paper Name	**Author**	**Year**	**Cloud**	**Platform**	**Tool or Strategy**	**Notes**	
						Advantage	**Limitations**

			Service				
Forensic Acquisition of Cloud Drives	VassilRoussevy, Andres Barreto, Irfan Ahmed	2016	Google Drive Microsoft one drive Dropbox Box	Mac or Windows system	Design & Implementation of new acquisition tool kumodd.	Introducing a new tool kumodd which can perform cloud drive acquisition from four main providers.	Kumodd cannot acquire cloud native artifacts in their original format as they are not portion of the official API supported.
Cloud Storage Client Application Evidence Analysis on UNIX/Linux	R. Malik1, N. Shashidhar1, and L. Chen2	2015	Dropbox ownCloud	Ubuntu 14.04 Android OS	Methodology is to use different programs, tools and command line.	This research highlighted that numerous evidence can still be found on the Ubuntu system when application is uninstalled.	The tools used to analyze does not have a valid counterpart for UNIX or Linux, then a dynamical analysis is used in collecting evidence which is harder.
Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform	R. Malik, N. Shashidhar, and L. Chen	2015	Dropbox ownCloud	Windows 8.1	Methodology is to use different tools and software programs such as SQLite Browser , Process Monitor , Process Explorer RegScanner, TSK toolkit.	This research proved that a lot of files are affected during installing the application, and others files are left behind during the uninstalling process.	Forensic analysis focused on (server side) of the cloud.
Cloud Storage Forensic: hubiC as a Case-Study	Ben Blakeley, Chris Cooney, Ali Dehghantanha, Rob Aspin	2015	hubiC	Windows 8.1	investigating the Access VM (1.1), Upload VM (1.2), Download/Open VM (1.3), Delete VM (1.4), Install Desktop VM (1.5), Upload Desktop VM (1.5.1), Uninstall Desktop VM (1.5.1.1), Download Desktop VM (1.5.2) and Delete Desktop VM (1.5.2.1)	These present significant risks to the secure use of the hubiC system both while the client is installed and after it has been uninstalled.	- Limited to Microsoft Windows version 8.1 only. - Can be Extended to applications of other categories of forensics techniques as cloud malware forensics, mobile device cloud applications forensics.
Paper Name	**Author**	**Year**	**Cloud Service**	**Platform**	**Tool or Strategy**	**Notes**	
						Advantage	**Limitations**

Digital forensic investigation of cloud storage services	Hyunji Chung, Jungheum Park, Sangjin Lee, Cheulhoon Kang.	2012	Amazon S3 Dropbox Evernote	Windows XP, Vista MAC OS Android	This paper has described a previously unknown method for forensic analysis of cloud storage services for various operating systems. Procedure for investigation of cloud storage service is illustrated in a graph in the paper which helps in investigating of cloud storage services.	Proposing a model of process for forensic investigation and Providing unknown method for forensic analysis of cloud storage services which help in the investigation of cloud storage services.	This paper doesn't focus on physical memory.
Google Drive: Forensic analysis of data remnants	Darren Quick ,Kim-Kwang RaymondChoo	2013	Google Drive	Windows 7 iOS 4.2.1	The methodology involves the following steps: 1.Commence (scope), 2.Prepare and Respond, 3.Identify and Collect, 4.Preserve (forensic copy), 5.Analyze, 6.Present, 7.Feedback, and Complete. This	In the context of this research, the data created and used may be required in future research opportunities, and hence has been stored on multiple hard drives to enable future use.	This research was limited by not able to install the Google Drive application or to jailbreak the iPhone.
Windows 8 Cloud Storage Analysis: Dropbox Forensics	S. Mehreen, B. Aslam	2015	Dropbox	Windows 8	The methodology consists of four steps identify, preserve, analyze and present.	It could be of considerate value for the developers of this application for up gradation of security features.	No DLL files exists for metro application which means that application bypasses the firewall and connecting to the server, investigating the password of the account not covered
SugarSync forensic analysis	Mohammad Shariati , Ali Dehghantanha& Kim-Kwang Raymond Choo	2015	SugarSync	Windows 8 MAC OS 10.9 Android 4 IOS 7	Methodology is to use different tools and software programs such as Regshot 1.9.0, Process Monitor 3.05, Nirsoft web browser passview1.43	Examiner allowed to extract SugarSync credentials, method of access, filenames and associated metadata when SugarSync is used.	Virtual environment limitation. The tool used (Digital Detective Net Analysis) hadn't the ability to run on virtual environments.
Paper Name	**Author**	**Year**	**Cloud**	**Platform**	**Tool or Strategy**	**Notes**	
						Advantage	**Limitations**

			Service				
Amazon Cloud Drive forensic analysis	Jason S. Hale	2013	Amazon cloud drive	Windows XP SP3 Windows 7 Professional 64-bit SP 1	Methods used in research : 1- Determining what file was transferred to or from an Amazon Cloud Drive. 2- Determining (date and time) that files were transferred to or from an Amazon Cloud Drive will be dependent on the method of transfer used and the level of access.	Two Perl scripts were introduced to ease the time and effort that would be required to parse the information.	Google chrome wasn't significantly tested because of the fact that latest versions of the browser are reported that are incompatible with the online interface of Amazon Cloud drive.
Digital droplets: Microsoft SkyDrive forensic data remnants	Darren Quick , Kim-Kwang Raymond Choo	2013	SkyDrive	Windows 7 PC Apple iPhone 3G	The methodology involves the following steps: 1.Commence (scope), 2.Prepare, 3.Identify and collect, 4.Preserve (forensic copy), 5.Analysis, 6.Presentation	Providing case study that outlines where the information previously identified, assist in an investigation, and also follows the proposed Digital Forensic Analysis Cycle.	This research wasn't able to jailbreak the iPhone.
A forensically robust method for acquisition of iCloud data	Kurt Oestreicher	2014	iCloud	MAC OS 10.9	The methodology involves these following steps : 1. Initial configuration. 2. Data Collection. 3. Analysis.	This paper first examines similar cloud research that has been conducted on other platforms. A methodology for validating the iCloud acquisition process is then explained in detail.	This paper does not explore the incorporation of iOS devices as (iPad or iPhone) in the iCloud synchronization schema and any affect that iCloud has on files synched through these devices.
Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?	Darren Quick, Kim-Kwang Raymond Choo	2013	Dropbox Google Drive SkyDrive	Windows7 Home Basic	Cloud Storage Data Collection strategy 1. Identification. 2. Preservation. 3. Analysis. 4. Presentation	The researchers verify their finding through conducting an analysis using commercial forensic tools such as namely X-Ways, AccessData Forensic Toolkit.	New release of client software may change the way the files are downloaded in future, which may affect the associated dates and times.