Extracting Potential Forensic Evidences from Cloud Client Device using own Cloud as a Case Study

Ghania Al Sadi
Sohar University, Computing Department
Sohar, University Rd, 311
Sultanate of Oman

ABSTRACT
The highly distribution of cloud storage as a mean to store data rises the need to find a suitable forensic methods to extract forensic evidences during investigating criminal or illegal activities on cloud accounts. Most accurate evidences can be extracted from cloud serves; however forensic investigators cannot grant access to cloud servers due to privacy policies followed by cloud providers. Actually, amount of evidences can be extracted from client devices that may be of forensic investigator's interests. This research utilizes open source cloud software to study cloud client structure to extract potential evidences from cloud client devices that will serve cloud forensic investigation field.

General Terms
Cloud Computing, Cloud Storage, Forensic Investigations

Keywords
Cloud Storage, Cloud Forensic, Cloud Client, Forensic Framework, Potential Evidences

1. INTRODUCTION
Cloud Storage is one of the cloud service models that is referred to as Storage as a Service (StaaS). It accommodates a logical pool of storage to store data through a range of devices. StaaS is highly distributed compared to other cloud models due to its importance in storing data that can be accessed remotely anywhere and anytime using different synchronized devices. Many cloud vendors provide a free amount of cloud storage with different options for different types of customers. Users can increase the provided storage capacity based on their demand with charge that is specified by cloud provider (Martini and Choo 2013). Typically, StaaS is owned and controlled by organizations that host the service and are responsible for managing the physical cloud infrastructure. Cloud storage owners must ensure meeting storage requirements including availability of data, reliability, high performance, consistency and replication to provide a complete storage system. However, most cloud systems find it difficult to meet all these requirements together (Wu et al. 2010).

Cloud storage has a number of features that make it a more effective way for storing and retrieving data for both individuals and organizations. Cloud storage provides features to facilitate copy, backup, synchronization and file sharing where all these features are utilized using any device, at anytime and anywhere (Borgmann 2012).

- **Copy** - This feature ensures the availability of data in cloud server even in case of hardware failure like hard disk crash or stolen devices.
- **Backup** – Cloud storage keeps old versions of a file stored in cloud for a long period of time that can be easily recovered later. Backups are automatically created on cloud storages. Usually, cloud providers offer backup software that is installed on client device to backup data and configure backup options like backup schedule, monitor process and restore history.
- **Synchronization** – This feature ensures the consistency of data stored on cloud that is accessed using different type of devices. Also, synchronization ensures that any change made on a specific file using a particular device will be available on all other devices used to access that file. Moreover, it prevents conflict occur on data if same data has been changed using two or more different devices at same time.
- **File Sharing** – Sharing files over cloud storage is enabled for users to share data with others. Users sharing files can get different types of permissions over the shared files like read, write, update, upload and delete rights.

Generally, cloud storage features are the reasons of its popularity in cloud computing community. It is more flexible than the traditional storage devices and it is more efficient in many cases that can be faced by different level of users. By using cloud storage, users can access their data from any location using different type of devices like mobile device, laptops or desktops. Also, with cloud storage, users can have a copy of a high amount of data without the need of copy their information on storage devices like hard disks or Flash Memories. Copying data to cloud storage eliminate losing data in case the storage devices are stolen or lost.

As with all computing systems, cloud security can be broken by criminal activities to obtain unauthorized access to cloud data. Generally, cloud is more attractive by attackers because it is running over the internet and can be accessed anywhere using any synchronized device. Actually, cloud synchronization raises the chances for attackers to exploit cloud to practice illegal activities on data. As defined, by the European Network and Information Security Agency (ENISA) report in 2012, cloud providers are not responsible to provide access to their servers to obtain raw log data for forensic analysis in case of compromising cloud accounts because cloud uses multi-tenant model and store data on a shared storage pool (Martini and Choo 2013). So, providing such data for forensic investigation purposes will compromise other users' data while data are stored on a shared pool of resources. Therefore, finding a suitable forensic techniques is highly recommended to accommodate the rapid growth of cloud computing.

2. CLOUD FORENSIC
In traditional digital forensic, the investigators have the opportunity to seize a device and examine storage elements to extract and recover evidences. In cloud systems, investigation process may take another pathway since it has a different architecture that is considered as a complex architecture.

Technically, cloud system based on virtualization that allocate cloud resources to different virtual instances assigned to different clients where a number of users can share a same physical infrastructure. Clients then can access data remotely via internet using any synchronized device to store and retrieve data (Sabahi 2011). Virtualization maximize the difficulty of conducting forensic investigation on cloud because client's data is logically stored on client accounts but it is physically stored on server' datacenters. Therefore, forensic investigators miss the accuracy of finding the actual device used to compromise any cloud account since data are physically available in cloud servers (Haggerty 2013).

Cloud servers contains a high amount of data in its shared pools related to many users, thus trying to seize cloud servers will affect the privacy of users' data stored on the same cloud. Therefore, in most cases granting access to cloud servers is not visible. Even though, forensic investigators can obtain data logs from cloud providers, but normally the provided evidence will not be as accurate as expected when it is collected by investigation experts (Zawoad and Hasan 2013). This assumption maximizes the need to seize cloud storage servers to conduct forensic investigations. However, forensic investigators don't have legal access to cloud datacenters and servers that are owned by cloud providers to collect forensic evidences in criminal cases. Moreover, cloud synchronization is considered as another difficulty faced by forensic investigators because they miss the opportunity to seize a suspected device while cloud data can be accessed using different synchronized devices from anywhere and anytime. This feature minimize the chance of finding the exact device used to access any compromised account therefore, data logs are required during this process to find synchronized devices' details like IP addresses (Birk and Wegener 2011). Thus, conducting forensic investigation on cloud servers is highly required to collect accurate data. However, amount of potential evidences can be left on client devices by criminals.

Traditional forensic techniques can be applied to investigate cloud criminal cases but the accuracy of evidences cannot be maintained due to absence of physical storage devices. However, forensic investigators apply traditional digital forensic techniques while investigating cloud criminals due to the lack of cloud forensic techniques. In fact, the rapid growth of cloud computing limits the ability to find an advanced forensic technique to apply during investigating cloud criminals. Generally, network forensic is considered as a suitable forensic technique to apply on cloud forensic investigation since cloud computing based on network access. Cloud forensic may require investigating memory processing, registry files, network logs, histories and file systems (Zawoad and Hasan 2013).

Technically, conducting forensic investigation on cloud computing requires client artefact and cloud server artefact depending on the cloud model. For example, in private cloud investigating both artefacts is reasonable while it is not applicable in public cloud due to lack of access to cloud service provider servers. Regardless of accessing the cloud server, a number of potential evidences can be collected from client device as defined in this research.

3. CLOUD FORENSIC INVESTIGATION FRAMEWORK

Typically, to start the investigation process, a forensic framework is required to go through the investigation process step by step. Generally, conducting cloud forensic requires an advanced framework that differs from that is used in traditional forensic investigation to suite the nature of cloud environment. As mentioned previously in this research, cloud computing based on network access, therefore cloud forensic is stated as network forensic. As stated by United Nations Office on Drugs and Crime (UNODC), the effective investigation on internet activities based on a combination of traditional investigation methods and techniques, the availability of the correct tools, and the correct decision taken to prosecute the criminals in such cases (Council of Europe 2007).

Since, cloud computing is a new technology deployed in the recent years, then there is a limited number of researches discussed forensic investigation frameworks on cloud. One of the suitable cloud forensic investigation frameworks is proposed by Ben Martini and Kim-Kwang Raymond Choo in 2012 that integrates two of the widely used frameworks on conducting digital forensic. The framework combines NIST framework and McKemmish (1999) framework to provide an integrated conceptual digital forensic to support forensic investigation on cloud (Martini and Choo 2012). Although the integrated framework is a combination of two frameworks, it has a main difference that based on the iteration. Iteration allows the investigators to return back to previous stages during investigation process to collect more evidence (Martini and Choo 2013).

The integrated framework consists of four phases that combine both NIST and McKemmish (1999) phases as shown in Figure 1.

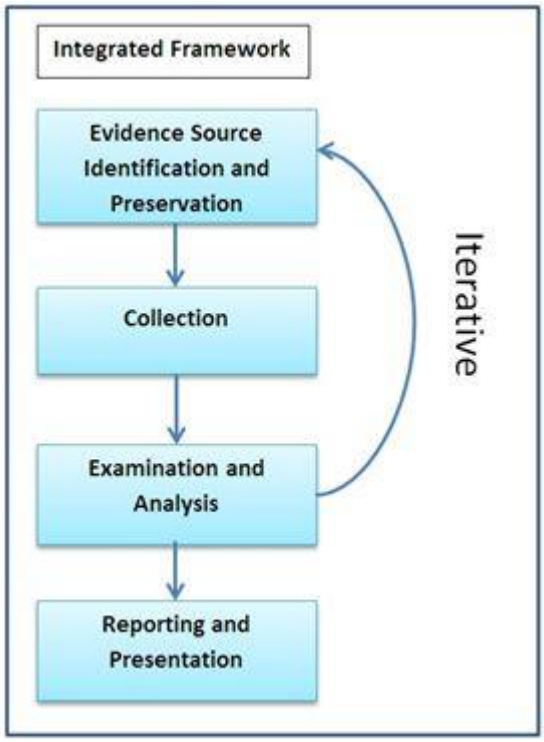

Figure 1: An integrated conceptual digital forensic framework for cloud computing

4. FORENSIC INVESTIGATION EXPERIMENT

The research is using ownCloud service as a case study to conduct the research to support digital forensic strategies employed on cloud environment. During research, client artefact is investigated to extract potential evidences left on

client device by criminal. Moreover, the research explore potential issues that may be available in public cloud storage that will help to obtain the required data for digital forensic investigation and at the same time provides recommendation for those who intent to utilize private cloud storage to store their valuable data.

4.1 Own Cloud Overview

ownCloud software is a free open source software developed to simulate public cloud storage such as Dropbox. ownCloud provide all cloud storage capabilities to store, manage, modify and retrieve data. It is a safe and secure environment that provides file synchronization and sharing capabilities on own servers under the organization control. Different types of files can be stored, managed and shared easily in ownCloud storage. ownCloud storage can be accessed using different types of devices like laptops, desktop, tablets and smartphones. ownCloud storage can be accessed via web browsers or client application. It supports sharing data among users either in private network with subscribed users on ownCloud or other external users in public network. It provides storage service over APIs to enhance customization capabilities and meet users' requirements (Hani et al. 2014).

ownCloud software is composed of server software that is running on cloud environment and client software that consists of ownCloud sync client application and web interface. OwnCloud enable mounting any storage protocol to the server like NFS, GFS2 and clustered file systems to enable a wide range of storages. Also, external file system applications can be mounted to ownCloud server like WebDAV, Windows Home Directories, FTPs, Google Drive and Dropbox. A various number of open APIs included in ownCloud to be integrated with other systems. On the other hand, ownCloud deploy a powerful API for users to enable accessing to ownCloud data. Users can access ownCloud via web interface or WebDAV to view, share and sync data among different devices. A number of productivity features included within ownCloud client interface to enhance and simplify user activities like view, upload, download, edit and delete data.

4.2 Cloud Client Forensic

Cloud forensic is considered as network forensic, so live forensic is most suitable to conduct investigation analysis on most given cases like deletion or modification of data. Live forensic captures network, browser's artefact and memory data that could not be captured from memory images (Martini and Choo 2012). A number of artefacts will be analyzed on the client devices like ownCloud Synced Folder, ownCloud web client Interface and network analysis to extract evidences that may be linked together for more accuracy.

Based on cloud forensic framework, investigation process will go through defined steps to extract and analyze evidences depending on a given criminal case. In each forensic framework, identifying evidence source is the first step that should be conducted to find a suspected device to seize for investigation purpose. While seizing suspected device, investigators must ensure integrity of data by preserving evidence and prevent any change on data. In case of cloud criminals, a suspected device must be seized and the compromised cloud account must be frozen to ensure integrity of data. Collecting and acquiring the required evidences from the seized device comes as a second step during digital forensic investigation process. A number of forensic techniques can be used to acquire data during this phase. However, live forensic is the only suitable technique that can be used to collect data from cloud artefact where collecting data from disk image is not enough to decide on any cloud's criminal case (Martini and Choo 2012).

A number of artefacts can be analyzed on the client devices like cloud Synced Folder, cloud web client Interface and network. Moreover, some potential evidences can be collected from memory capture, network captures and browser artefacts. During investigation process, analyzing the collected data sources is considered as an important phase to find the accurate evidences on the case. A suitable forensic toolkit is required during this phase that must suit the used digital forensic technique. The expected output during this phase is to check and assure the occurrence of any criminal case on cloud accounts by examining all available cloud components on client device.

4.3 Forensic Examination and Analysis

This research found a number of cloud components that contains some potential evidences that can be linked together to get accurate evidences to be accepted by law enforcement agencies. All available components are analyzed 'as following using live forensic model to extract the required evidences:

- **Client ownCloud Folder** - Technically, when installing ownCloud client software, a synced folder is created on the location ***"C:\Users\..\ownCloud"*** which contains all user files stored in ownCloud instance where it can be used to store, delete and modify files that are automatically synced with ownCloud account. By analyzing the folder, ***"owncloudsync.txt"*** file is found as a hidden file that consists of all activities occurred on the ownCloud account. The deletion activity is shown in a clear text in the file with the deleted file name and time as shown in Figure 2.

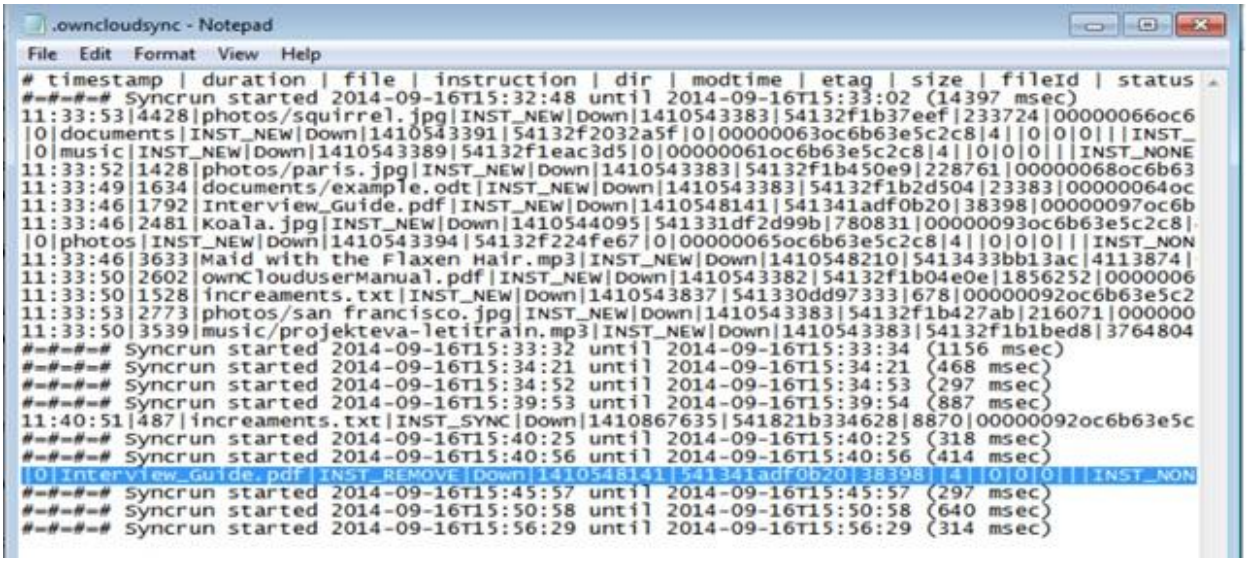

Figure 2: owncloudsync.txt file that contains all activities occurred on ownCloud account

- **Own Cloud web client interface** - Client interface can be accessed using any desirable web browser. The interface enables the user to upload, download, modify and delete files. Deleted files are temporarily deleted to Deleted files folder that allows the user to recover files again. When files are deleted from Deleted files directory are permanently deleted and cannot be recovered using client interface. However, investigators can utilize some professional software to recover deleted data only from the device used to delete the file because deleted data may still be accessible in the memory capture. The key challenge is that data can be deleted from any synchronized device but it can be recovered only from the device deleted from since data are physically stored on cloud servers. Therefore, it is difficult for forensic investigators to recover data deleted during criminal cases by utilizing any other synchronized device. Moreover, ownCloud provide file versioning feature to store multiple versions of a modified file and enable restoring the old versions again as shown in Figure 3. It is a beneficial feature for forensic investigators which enable determining the potentially modified files whereas it provide the time of modification.

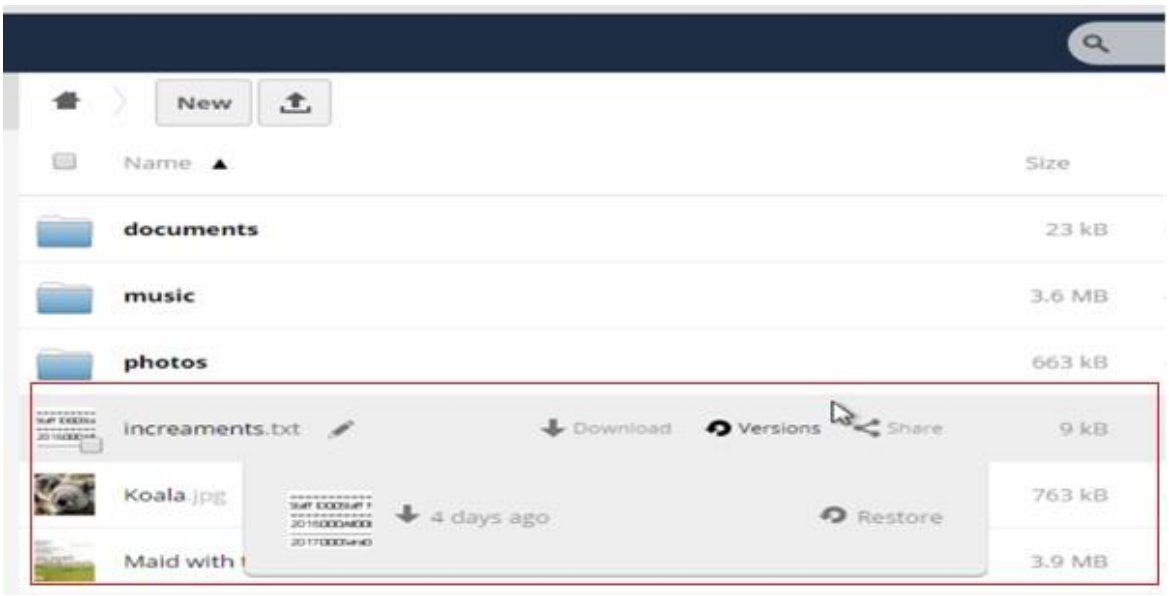

Figure 3: File versioning feature on ownCloud

- **ownCloud Activity App** - All recent activities on the account are displayed in the activity log. As show in Figure 4, the deletion, modification actions are clearly stated with the file name and time. But the limitation is that the synced device details used to access the cloud account are not exists. For example, the deleted PDF file exists in the log with time of activity occurrence as shown in the figure below.

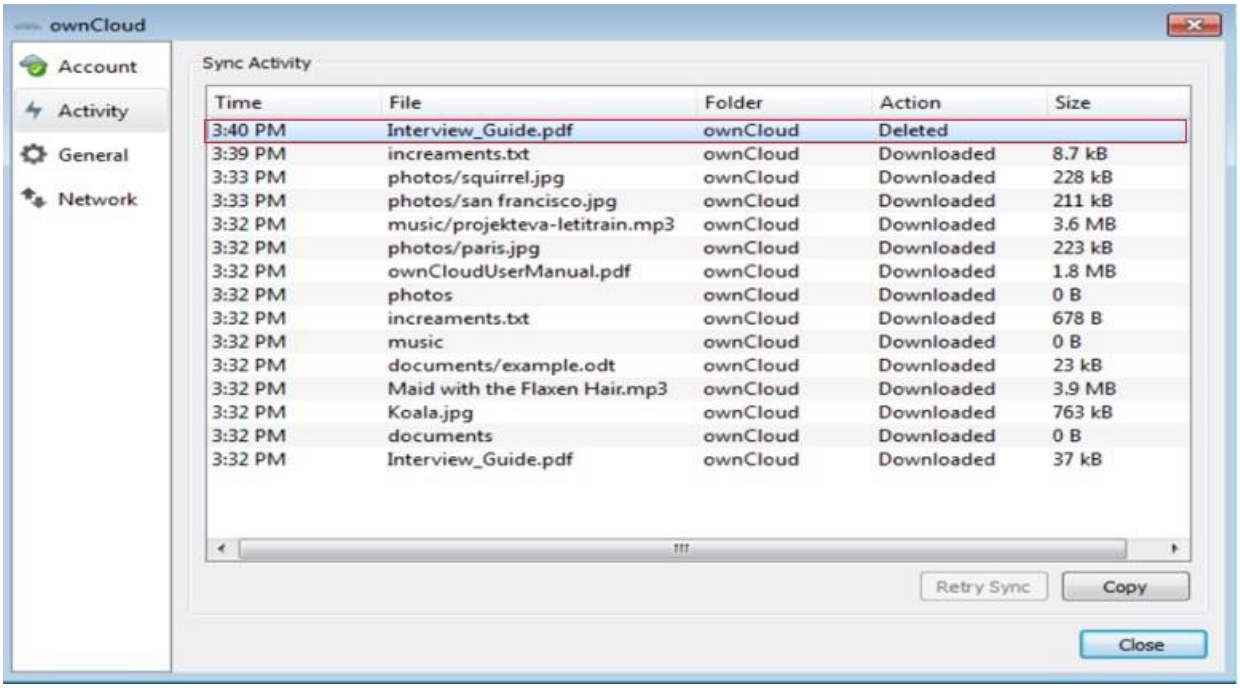

Figure 4: ownCloud Activity App

- **Network analysis** - The packet captures will be utilized to analyze the communication between the client and server on the ownCloud system. A number of browser forensic tools can be utilized to intercept the HTTP traffic. The obtained result from this analysis shows some required details where all visited URLs are captured along with page title, visited time, number of visits and other related information. As illustrated in Figure 5, the ownCloud web interface was accessed multiple times and multiple page of the web interface was browsed like Deleted Files page, Files page and other pages. However, unfortunately the user credentials are not shown to determine the authentication details of the users. Intercepting network packets is an important process conducting during investigation criminal cases on cloud system while cloud accounts are accessed via internet. It enables investigators to match all extracted evidences from all cloud components to provide accurate conclusion. The figure below shows the evidence linking process that link the captured network packet with evidences collected from the Activity App. As shown, the occurrence time of deleting the PDF file match the time of browsing Deleted files page on ownCloud web client interface as collected from network captures. This conclusion ensures that the suspected device was utilized to delete the file from the cloud account.

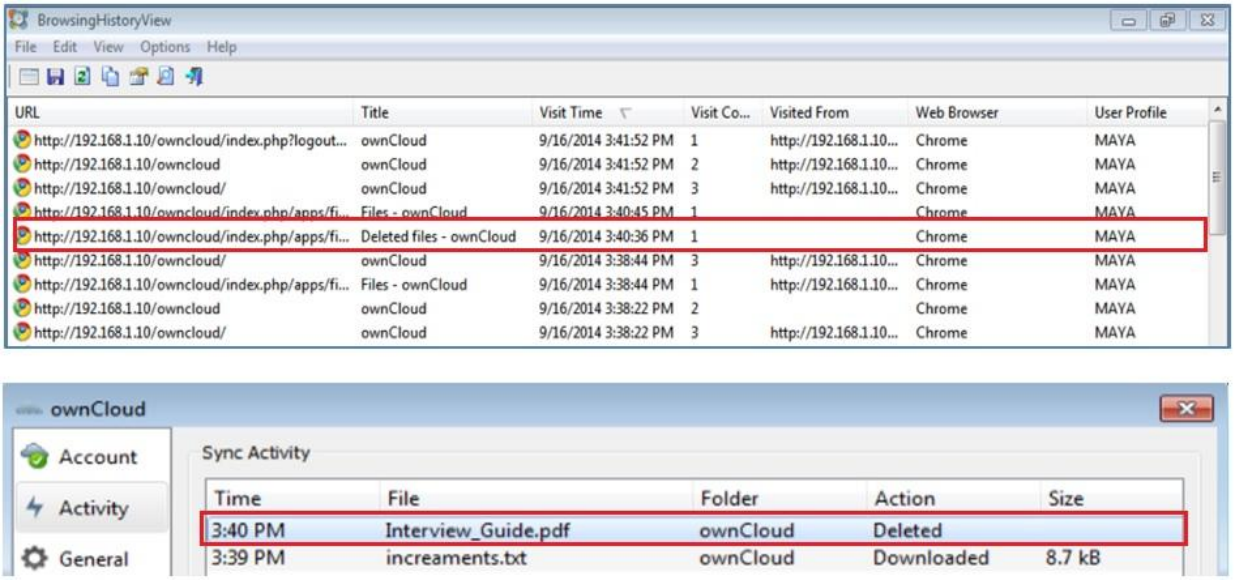

Figure 5: Linking extracted forensic evidences collected using different tools for accuracy

- **owncloud.cfg file** - The file consists of the user authentication details owning the installed ownCloud application. The file is required in the analysis process to determine the actual user of the ownCloud Client application installed on any suspected device. As shown in Figure 6, the authentication details are related to the user ***"sara"*** that configured on a device is related to another user. This leads to a conclusion that may criminal utilized login details of another user to grant access to cloud account by installing cloud application and configuring the account using a victim's authentication details and therefore trace all the synced activities occur on the account and use the stored files.

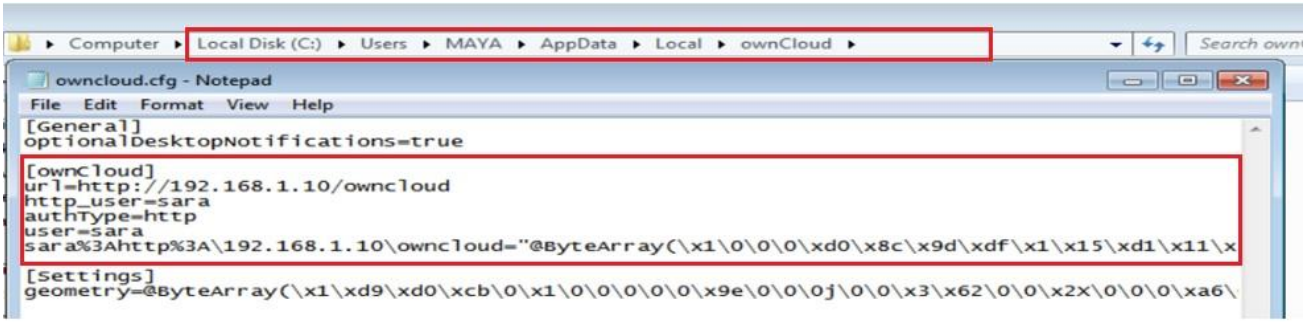

Figure 6: ownCloud's User Authentication File

When proving that the file is deleted from the suspected device, then a recovery method will be used to check the ability of recovering files deleted from the ownCloud account. Generally, deleted data can be obtained from memory capture on the same device. Therefore, recovering data from the same device used to delete cloud files is more reasonable by utilizing some powerful tools.

The below table provides a summary of all the data required by investigators to conduct forensic investigation on ownCloud client. Investigators can extract more potential evidence that may be of their interest to be linked to ownCloud instance and search for more and accurate evidence. For example, authentication details can potentially help the investigators to link user activities with the stored files in the ownCloud storage based on timestamp.

Table 1. Own Cloud Client Artefact Summary

Analyzed Artefact	Location	Description
ownCloud Client Folder	C:\Users\..\ownCloud	Consist of all synced files stored in ownCloud storage that help the investigator to check what files stored in the ownCloud instance.
owncloudsync.txt	C:\Users\..\ownCloud\owncloudsync.txt	Located in ownCloud folder as a hidden file that shows a log and metadata of account activities. It supports the investigator to determine what actions have been conducted on the user files stored on ownCloud instance and at which time.
ownCloud Sync Activity	ownCloud Interface Application	Shows a log of all synced activities occurred on ownCloud account.
Deleted Files	ownCloud web client Interface	Consists of the files deleted by the user and allow to restore files again while are still exists on the Deleted Files directory.
owncloud.cfg	C:\Users\SARA\AppData\Local\ownCloud	Shows the authentication details of the client and user credentials if stored. It helps the investigators to determine the authenticated user of the available ownCloud instance.

5. CONCLUSION

Considering public cloud storage model, clients has no control over the storage infrastructure to manage configuration of storage, network or applications. The client has only limited control over the stored data and some applications used to view these data. Therefore, only limited evidence can be collected when investigating criminal cases. Normally, the collected evidence from client side is insufficient to provide a complete report for judicial systems. Also, a clarification is required to illustrate data recovery techniques in case of losing data on cloud. Moreover, to define criminals, it is important to find information like IP addresses related the synchronized devices used to access cloud account from different places. To obtain this type of information, investigators need high-level logs that are obtained from cloud servers and provided by Cloud Service Provider. Also, to collect evidence from cloud storage accounts, account's activity logs are required to track all events occurred on the account like open, upload, download, modify and delete files. As stated before, the accurate and detailed logs can be obtained from cloud provider even though some logs may be obtained by scanning client web browser. Typically, the secure source of cloud evidence is essential of forensic investigation success. However, this source is only available in provider's storage servers that include meta-data and history of cloud digital objects. Thus, most researches

recommend interested organization on cloud storage to configure private cloud storage to minimize both security issues and forensic investigation limitation. An advanced cloud forensic techniques may be the main aim for future researches in cloud forensic area. The technique is required to obtain accurate details of the synced device used to access cloud accounts for illegal purposes. This technique should be an extra feature provided for client accounts.

6. REFERENCES

[1] Birk D, Wegener C. Technical Issues of Forensic Investigations in Cloud Computing Environments. 2011 Sixth IEEE Int Work Syst Approaches to Digit Forensic Eng [Internet]. 2011;1–10. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6159124

[2] Borgmann M. On the Security of Cloud Storage Services. 2012;1–146. Available from: papers3://publication/uuid/FE433248-1727-4313-A988-9EFC0E1B7CE9

[3] Council of Europe. Cyberterrorism: The Use of the Internet for Terrorist Purposes. 2007;497.

[4] Haggerty J. Digital Forensics in the Organisation. 2013;(October):17–20.

[5] Hani AFM, Paputungan IV, Hassan MF, Asirvadam VS, Daharus M. Development of private cloud storage for medical image research data. 2014 Int Conf Comput Inf Sci [Internet]. 2014;1–6. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6868433

[6] Martini B, Choo K-KR. An integrated conceptual digital forensic framework for cloud computing. Digit Investig [Internet]. Elsevier Ltd; 2012;9(2):71–80. Available from: http://linkinghub.elsevier.com/retrieve/pii/S174228761200059X

[7] Martini B, Choo K-KR. Cloud storage forensics: ownCloud as a case study. Digit Investig [Internet]. Elsevier Ltd; 2013;10(4):287–99. Available from: http://linkinghub.elsevier.com/retrieve/pii/S1742287613000911

[8] Sabahi F. Cloud computing security threats and responses. 2011 IEEE 3rd Int Conf Commun Softw Networks. 2011;245–9.

[9] Wu J, Ping L, Ge X, Wang Y, Fu J. Cloud Storage as the Infrastructure of Cloud Computing. 2010 Int Conf Intell Comput Cogn Informatics [Internet]. 2010;380–3. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5565955

[10] Zawoad S, Hasan R. Digital Forensics in the Cloud. CrossTalk [Internet]. 2013;(October):17–20. Available from: http://www.crosstalkonline.org/storage/issue-archives/2013/201309/201309-Zawoad.pdf