Analyzing Data Remnant Remains on User Devices to Determine Probative Artifacts in Cloud Environment

Abdulghani Ali Ahmed,[1] PhD.; Chua Xue Li,[1] BSc

[1]Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Pahang, Malaysia.

*Funding support was provided by the Ministry of Higher Education in Malaysia (No. FRGS/1/2016/ICT03/UMP/02/1), and the fund of COMSTECH-TWAS joint research grants the program for young scientists in OIC countries No. 14-340 RG/ITC/AS_C.

ABSTRACT: Cloud storage service allows users to store their data online, so that they can remotely access, maintain, manage, and back up data from anywhere via the Internet. Although helpful, this storage creates a challenge to digital forensic investigators and practitioners in collecting, identifying, acquiring, and preserving evidential data. This study proposes an investigation scheme for analyzing data remnants and determining probative artifacts in a cloud environment. Using pCloud as a case study, this research collected the data remnants available on end-user device storage following the storing, uploading, and accessing of data in the cloud storage. Data remnants are collected from several sources, including client software files, directory listing, prefetch, registry, network PCAP, browser, and memory and link files. Results demonstrate that the collected remnants data is beneficial in determining a sufficient number of artifacts about the investigated cyber crime.

KEYWORDS: Forensics Science, Digital Forensic, Cloud Storage, Cybercrimes Investigation, pCloud, Evidence Collection, Data Remnants, Artifacts

Cloud computing provides businesses and individuals different types of computer services. Organizations rely on cloud computing resources to replace large in-house computing systems, such as servers and data centers, to increase service accessibility and availability. These resources enable users to upload their data to servers, allowing them to access and share data with other users at any time.

Businesses can use computing services without high deployment costs through cloud computing. The high scalability of infrastructure resources provide businesses and IT organizations with increased opportunities for developing high-end, low-cost computing services. Pay-as-you-go models reduce computing costs. Businesses and organizations are provided many choices in cloud service providers to weigh advantages against possible drawbacks. These include losing control of personal computing resources, applications, and data storage.

Several studies and surveys have reported that cloud computing is subject to exploitation by malicious users despite the rapid advancement of cloud computing services. Loss of control over stored data is a security challenge in cloud computing. The authors in (1) concluded that the location of data storage in the cloud and the multi-tenancy of customers on cloud servers are security concerns. Forensic practitioners also face challenges from cloud technology because data can be accessed by malicious users using web browsers and portable devices without leaving traceable evidence. Dropbox™, iCloud, Mega, Tresorit, Copy, and Box are examples of cloud service providers that require further investigation.

Cloud computing means the use of a network of remote servers and data centers hosted on the Internet in different locations to store, manage, and process raw data. Cloud computing provide users with shared processing resources for computers and other devices connected to the network. Cloud storage service market has grown significantly (2). Forensic hand means the use of scientific tests or techniques for crime detection (3). Cloud forensics is a cross-discipline between cloud computing and digital forensics.

Cloud storage and its advancement bring advantages to computer users that are subject to misuse by irresponsible users and criminals, such as cases of criminals using cloud storage to store and exchange illegal material and to commit botnet attacks. The investigation process for extracting and collecting cybercrime evidence in cloud storage is tedious and challenging due to the increased complexity of each case. The seizure and evidence retrieval process for cloud digital forensics have encountered legal issues. Network World stated that businesses that use cloud computing should clarify with cloud storage providers their responsibility of providing forensic evidence in criminal incidents, such as cyber attacks or data breaches (4).

Users of public cloud services must cooperate with cloud service providers to obtain digital evidence because normal forensic investigators cannot obtain evidence from cloud service providers without proper warrants issued by a jury. Cloud service providers must carry out the evidence collection process on behalf of the requester to acquire

digital evidence. The forensic practitioners involved must ensure the authenticity and reliability of the evidence collected (5). They have difficulty gaining access to physical hardware to locate files and evidence because all data are stored in different data centers and computers worldwide. Data centers may not belong to the same entity or be located in the same country. Reference (6) stated that cloud systems and services give computer forensic practitioners difficulty in obtaining and analyzing digital evidence from traditional server-based systems due to such difficulty.

Having a proactive methodology is important to carry out digital forensic investigations that are sufficiently flexible to work with future providers of new cloud storage services (7). Forensics investigators must also have information regarding the location and type of data remnants left by cloud users from the devices they used to access cloud services (8). Forensic investigators must ensure that all digital evidence is acceptable and understandable by jurisdiction personnel that do not have IT backgrounds.

The present study reviews current challenges in cloud forensics and proposes a proactive scheme to improve the processes of locating and collecting cybercrime artifacts in cloud computing. This study investigates existing digital evidence collection methodologies using the data remnants left on user devices prior to the use of cloud storage applications. These data remnants are then used for new cloud storage development. Many online cloud storage services have been introduced to fulfill different customer demands. TABLE 1 provides a summary of some cloud storage providers.

TABLE 1 − *Summary of cloud service providers*

Feature	Dropbox	Google Drive	Microsoft OneDrive	pCloud
Size of free storage	2 GB	15 GB	5 GB	10 GB
Security	Client encrypted files, geo-redundant storage, and folder permission	Data stored encrypted in 128-bit AES	Encryption at rest is available on OneDrive for business users	Uses TLS/SSL encryption, applied when information is transferred from a device to the iCloud servers
File Versioning	Yes	Yes	Yes	Yes
Area of specialization	Compatibility with other services	Data syncing between devices	Collaboration with Microsoft Office 365	Valuable files are accessible even offline
File size restriction	10 GB with websites only	5 TB	10 GB	Unlimited
OS supported	Windows OS, Mac OSX, Linux OS, Android, iOS, BlackBerry, and Kindle Fire	Windows OS, Mac OSX, Android platform, and iOS	Windows OS, Mac OSX, Android platform, iOS, and Windows Phone	Windows OS, Mac OSX, Android platform, iOS, and Linux

Related Work

Section II reviews articles related to this study and discusses research findings, methodologies, limitations, and conclusions for each article. Quick and Choo conducted a study to determine ways to acquire files uploaded and accessed using Dropbox (7). A standard personal computer with a virtual machine (VM) was installed with the Windows 7 operating system; this was used to examine different cases using various PCs, as well as in the forensic analysis of Dropbox client software in different browsers. The browsers included Microsoft Internet Explorer®, Google Chrome™, and Mozilla Firefox®. This study determined the data remnants and artifacts left on a Windows 7 hard drive after using Dropbox. These data remnants include usernames, passwords, browsers, software access, data stored in accounts, and timeframes found on file metadata. Data from the Enron corpus was used to test accounts created with three service providers. MD5 values were created. VMs were made using VMware® Player 4.0.1. A VM for each service provider was used for testing, and Base-VM files were utilized as control media to discover newly created files after each scenario.

The network traffic generated by each scenario was observed using Wireshark. The timestamps of the original files were recorded, and the original files were hashed. Several files were uploaded from the Dropbox application, and copies of each browser were created and labeled. A similar process was completed when accessing and downloading files from created Dropbox accounts. All associated files from the Dropbox accounts were moved to the VM desktops as a zipped files. The zip files were extracted to the desktop, opened, and closed. The stored data was erased using the US Department of Defense 5220.22-M setting, which only deletes data after they are overwritten thrice (9).

The VMDK files of the VMs from the hard drive, along with each VMEM file and network capture file (PCAP), were identified for each VM for data identification. FTK imagers were used to capture data memory, and the remaining VMs were analyzed. The forensic copies were preserved and analyzed according to standard procedures. Eraser and CCleaner software erased the files on the cloud. The Dropbox application keeps a record of devices synchronized to an account. A timestamp of activities, such as the installation, uploading, downloading, and uninstalling of certain files and applications through Dropbox, was found. The hash values of each file remained unchanged. Thus, the data in the files were unaltered. The timestamps were manipulated by each service. Directory listing was produced using AccessData FTK Imager 3.1.0. Encase software was used to retrieve file names. The remaining files showed the Dropbox usage. Eraser or CCleaner software failed to completely clean the remaining

data on the use of Dropbox. Data concerning the previous presence of Enron or Dropbox sample files were completely removed.

Quick and Choo reported that several providers should be included in future research to determine whether files stored on their servers remain unchanged. Table 2 shows the contributions and limitations of their study. Dykstra and Sherman concentrated on the integrity of forensic data downloaded from Amazon Elastic Compute Cloud (EC2) servers (10). They investigated the accuracy of forensic toolkits in acquiring forensic data from cloud storage environments through the Internet. The study also expanded its research to live forensic acquisition using forensics tools, such as Fastdump from HBGary, Memoryze from Mandiant, and FTK Imager from AccessData. The percentage of success of the evidence collection process, the duration, and trust required was evaluated.

TABLE 2 - *Contribution and limitation of Quick and Choo's research*

Contributions	Limitations
Verified how to obtain the files uploaded and stored in Dropbox	Timestamps were manipulated by each service.
Revealed the data that remain on a Windows 7 PC using a Dropbox application. This includes the usernames, passwords, browsers, software access, remaining data stored in the accounts, and the timeframe found on file metadata	Only Dropbox was used in the case study, and the results cannot be proven to be the same for different service providers.

EC2 is an infrastructure-as-a-service solution, where clients have direct control over the establishment and usage of the VMs installed in a host server that enables forensic investigators to create a forensic image of the entire VM by uploading FTK or EnCase onto the VM. The created forensic images were examined using traditional forensic acquisition techniques. The manner in which remote forensic agent VM introspections were injected to remote acquisition was demonstrated.

Data from an EC2 VM were acquired using several techniques, such as using VMs to create forensic images. EnCase Enterprise or AccessData FTK was used to analyze the produced images. Other techniques include the use of Amazon Web Services to export data. Amazon exports requested data on an external drive and maintained a chain of custody. Amazon sends drives directly to the requestor along with a report of the exported data (10).

The study found that the files delivered to the requestor from Amazon have the same MD5 values as the original files. Therefore, the cloud data were not altered by the data acquisition process. Future studies were suggested to cover the request submission to Apple to export iCloud data to a physical drive for the requester. The data should be further analyzed to identify whether the metadata were altered from the initially uploaded files. TABLE 3 shows the contributions and limitations of Dykstra and Sherman's research.

TABLE 3 − *Contribution and limitation of Dykstra and Sherman's research*

Contributions	Limitations
Examined the forensic integrity of data downloaded from EC2 servers	This research is only applicable to EC2 servers. The results cannot be proven to be same using different service providers.
Investigated the ability and accuracy of forensic toolkits in the data acquisition process	Amazon exports the files to a physical hard drive that is sent to the requestor. This process may delay investigations.

Chung et al. (2012) conducted a study that focused on the data stored on servers (11). Chung stated that the difficulty in finding user activities upon service subscription is the most difficult aspect of investigating a cloud storage service (6). Information of user activities may be founded in the log files of a cloud server. However, most cloud companies are unwilling to release this information to protect the personal information and privacy of their clients. The study aimed to find traces left on PCs that access Amazon S3, Dropbox, Google Docs, and Evernote for cloud storage. The study also proposed a process for the forensic investigation of cloud storage services and described important elements of the investigation process.

Internet Explorer and Firefox were used to access clouds services in order to locate the data left in temporary logs files. Traces of system installation log and database files are left in the registry when installing an application on a Windows system. These files are vital because they contain traces of cloud storage service usage. Forensic investigators can obtain original documents and related metadata from the client device given that some cloud services sync the files stored on the cloud server with the computer's hard drive of the client.

The study included some constraints because it failed to compare MD5 values at each phase to show file integrity. The study's methods should be used as reference for cryptographic hashes to ensure that the files are identical. TABLE 4 shows the contribution and limitations by Chung et al.. Oestreicher (2014) also conducted a study that focused on data acquisition methods on iCloud (12) that locate iCloud-synched files in the operating system. The differences between the file acquisition process and the original files were used to identify hash value similarities and metadata to ensure file integrity for court presentation.

TABLE 4 − *Contribution and limitation of Chung et al.'s research*

Contributions	Limitations
Found files retained in PCs and smartphones after accessing cloud services from Amazon S3, Dropbox, Google Docs, and Evernote	The research did not compare MD5 values at each phase to show file integrity.

Proposed a process model for the forensic investigation of cloud storage services and described important elements of an investigation	The proposed model for the forensic investigation of cloud storage services should be further investigated using other providers of cloud storage service.

Two identical VMs were used to conduct the study: a subject computer and an examination computer. These VMs were clean and installed using Mac OS X 10.9. Various screenshots were taken at different stages to determine the location of artifacts formed by the iCloud service and to compare the subject and examination computers.

A new iCloud account was created on the subject machine, and the data was synced with iCloud. The second VM performed live data acquisition once synchronized with the newly created iCloud account. Data from file acquisition were analyzed to locate specific iCloud artifacts. The files were downloaded and compared with the hash value. The results showed that the data downloaded from iCloud were forensically sound. The similarity of the hashing value and the timestamps of the required data are important to prove the integrity of the acquired data. Oestreicher planned to find out whether the same results could be obtained using different models of Mac computers and different OS versions. TABLE 5 shows the contributions and limitations of Oestreicher's research.

TABLE 5 − *Contributions and limitations of Oestreicher's research*

Contribution	Limitation
Investigated the method of data acquisition on iCloud	Differences are observed in the MD5 hash values collected during experiments.
Located iCloud-synched files on the OS and the differences between the acquisition process files, and the integrity of the files acquired as evidence for presentation in court was identified.	The above technique only applies to iCloud storage on a secondary Mac OS X 10.9 machine.

Previous studies included a number of limitations. The cloud storage market consists of approximately 2,200 firms worldwide. Rather than focusing on well-known cloud storage services, such as Amazon, Google Drive, Microsoft One Drive, and Dropbox, research should be broadened to newly established cloud storage services to help forensic investigators obtain evidence from various cloud services. Different types of cloud storage services have different locations for data remnants stored in the computer hard drive after using the client software for cloud storage.

Collecting Cybercrime Evidences Scheme (Method)

This section aimed to identify and collect possible cyber crime evidence that could be found in the computer cloud storage. The method was designed using four components, which included the identification, locating, collection, and analysis of evidence, as shown in FIG. 1.

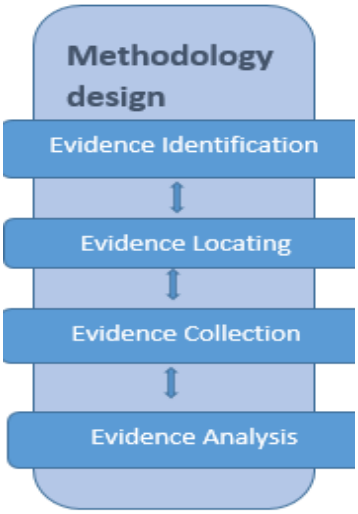

FIG. 1 − *Cybercrime evidence collection methodology*

An evidence identification component identified all the potential evidence of cybercrime. This component identified all the changes made during each executed process. The copied VM after each process was compared with the base VM to identify the file changes made to the registry and log files in each specific scenario created, for example, to identify each VMEM and VDMK files available and the database and logs files of the entire testing. Moreover, the relevance of peripheral components to the investigation must be considered. These components included the non-computer equipment associated with the targeted computer, such as printers.

An evidence locating process identified the location of each file change. This process served as a guideline in locating potential data remnants being stored. The evidence locating process was carried out by checking each potential location where the files reside in that the evidence can be copied and that evidence acquisition can take place. Evidence collection happens after the location of the data remnants was found. The images of the computer volatile memory (RAM) of each scenario and the VDMK files of each VM scenario were copied. AccessData FTK Imager Version 3.4.2.6 was used to obtain evidence.

The process was followed by the evidence analysis phase to determine what information can be extracted from each file. The analysis was conducted to compare the base image files to the subsequent image files copied in each scenario. This process determined the changes made. Observing the changes to the registry files and file systems was possible. This process recovered the evidence material using different methodologies, such as keyword search across the digital media, the recovery of deleted files, and the extraction of registry and log files information, as well as tools,

such as the SQLite viewer, HxD, AccessData FTK Imager, AccessData FTK, Wireshark, and Event viewer. FIGURE. 2 shows the flowchart of the overall process during the experiment.

Moreover, the flowchart was used to guide the conduct of planned experiment scenarios in order to achieve the desired result within a specific time frame. This process also provided an overview on how the experiment was conducted to avoid wasting time. Each process used the new VMs, which were copied, deleted, and reinstalled after testing to ensure that each scenario was created in a new VM environment and that accurate data were obtained. The following scenarios were carried out in the newly created VMs. FIG. 3 shows the usage of VMs when the scenarios were carried out.

The implementation stage required all the details gathered during the methodology design phase. The concluded steps were implemented in the real experiment. The experiment was carried out using the two VMs earlier mentioned to conclude the result. The two VMs were deployed to two computers for testing. All experiments can be implemented within the shortest time possible to avoid resource waste. The specific requirements and design specifications were studied briefly to ensure that all the processes can be carried out smoothly. All necessary software and hardware devices were prepared before starting the integration and system testing phase to avoid unnecessary problems that may disrupt the testing process.

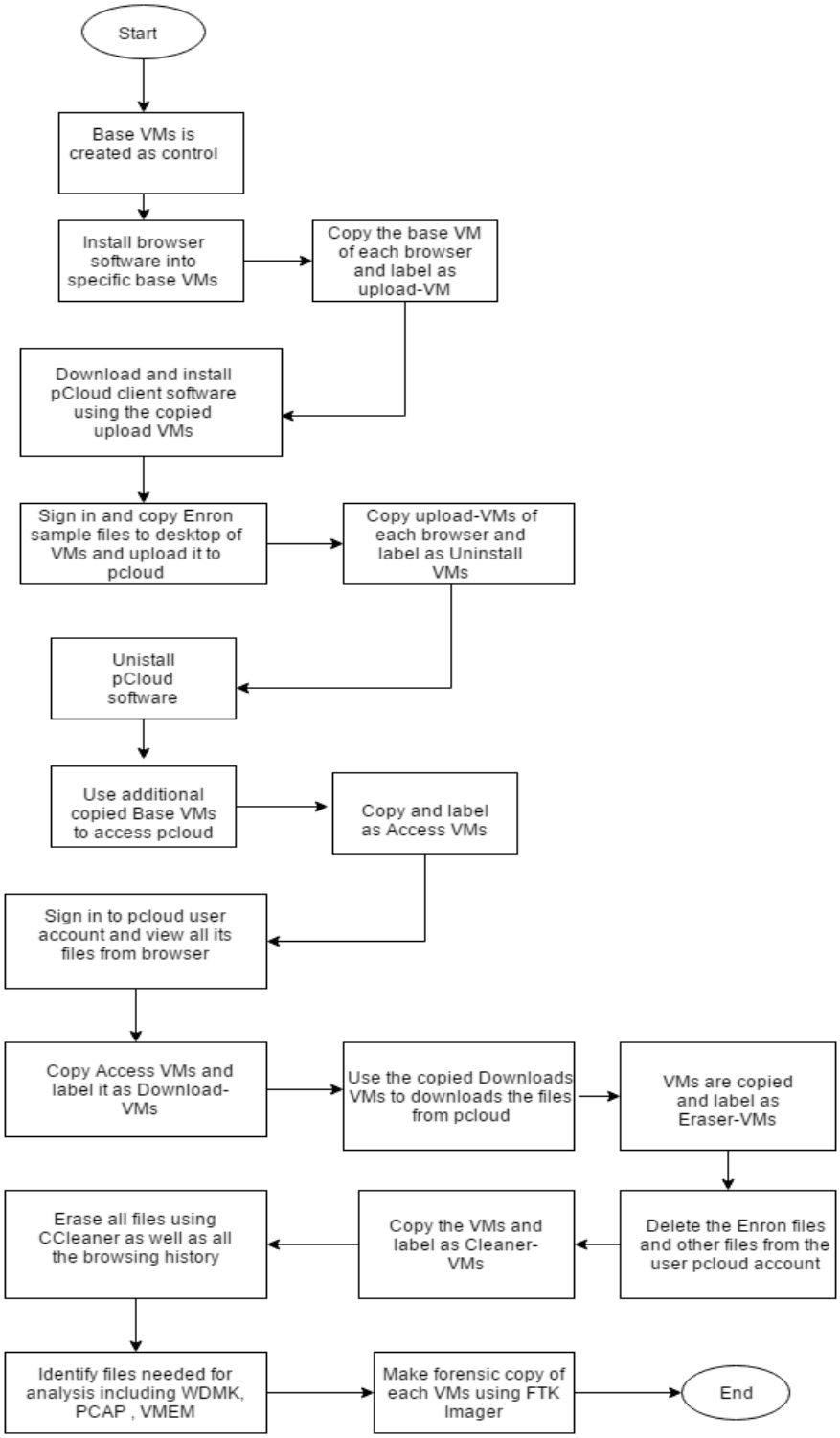

FIG. 2 − *Flowchart of cybercrime evidence collection*

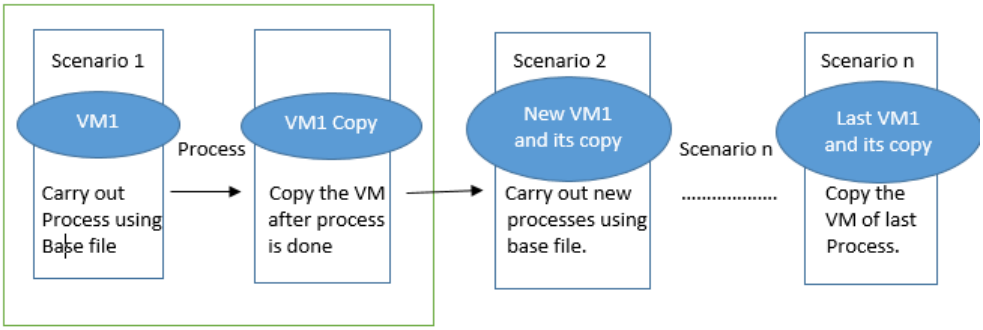

FIG. 3 – *VM usage when scenarios were carried out*

Experiment and Result Discussion

This section discusses the experiment and its results in detail, which include the steps and types of tests carried out. This scheme was implemented through the analysis of the web browser pCloud account information, control images created for each VMs scenarios, and pCloud client software. Moreover, the uninstallation process of the client software, directory listing, prefetch, registry, network PCAP, browser, memory, and link files were also analyzed and discussed.

Analysis of Files Created From Scenarios Carried Out and their Location

Each of the forensic image files retrieved from each scenario, as well as the network PCAP and memory dump files were copied from the hard drives. All forensic images copied were examined and analyzed using various tools, such as AccessData FTK Version 5.5, AccessData FTK Imager Version 3.4.2.6., HxD Version 1.7.7.1, and Wireshark network analyzer 2.0.5. The analysis processes were conducted to determine the content of data remnants created and left on the PC hard drives. These data remnants help forensic investigators in illustrating client activities and other necessary information.

pCloud account information using a web browser

When accessing https://my.pcloud.com/ using different web browsers, the username is displayed at the top right corner of the browser. The records of devices, which include mobile and PCs synced with the pCloud account, were shown with the number of spaces used and available for the user. Moreover, the details of the files and folders stored

were also written on the homepage of pCloud websites. They include the folder's last modification date and files size. Each file has a file info icon that allows the user to view the metadata of the files.

The account settings and download links, as well as the linked account settings can be changed at the top right corner of the browser. The account settings offer the option to show or hide system hidden files and to reset account passwords. Active tokens regarding the devices used to access the accounts and other related information, such as the creation and expiration dates, are available. An option to show download links separately along with detailed usage stats in download link settings is also available. Moreover, pCloud provides an option for users to back up their folders and files to other accounts, such as OneDrive, Facebook, Instagram, Dropbox, and Picasa Web Album accounts.

Accessing pCloud accounts using web browsers allow users to unlock pCloud's featured client-side encryption software, enabling users to manage and to prevent intrusion from unauthorized access and protect sensitive information and stored files. Users can have an encrypted folder for sensitive files. The features are available for users for $3.99 monthly. However, this special feature makes the process of evidence acquisition highly tedious because data can easily be hidden from the view of forensic investigators.

Accessing a pCloud account using a web browser also allows users to view deleted files in the Trash folder. Users can view their deleted files and restore their files when necessary in Trash. Additional information about the deleted files is available, such as the date and time the files were deleted.

The files in pCloud were stored in at least three different servers located in different data centers. This action ensures the redundancy of data. Thus, during server failure, users can still obtain their files from other functioning servers. pCloud provides offline access to users who do not have active internet connection. The information and metadata files in pCloud have their own purposes, which guide forensic investigators in obtaining crucial evidences of crimes.

Analysis of pCloud base images created by different browsers

Base images were created before each scenario is set to act as a control. This step ensures that related artifacts and files do not exist before each browser is installed and scenarios are carried out. To conduct the analysis, we ran keyword searches with the different terms shown in TABLE 6. The analysis indicated that data and artifacts related to browsers and pCloud client software files did not exist before each installation.

Analysis of pCloud client software

The results of the earlier test show that the pCloud client software was downloaded from www.pcloud.com for Windows 7. The downloaded files were stored in the "C:\Users\ [username]\Downloads\" folder with the name pCloud_Windows_3.3.1, which shows its software version. After running the program, a window instructed users to install Microsoft.NET 4.5.2 to continue the installation process. The same scenario occurred in the four VMs used for the installation process of the pCloud client software. After installing Microsoft.NET 4.5.2, the executable file pCloud_Windows.exe was copied to the hard drive of the VM created earlier.

TABLE 6 − *List of keyword search terms*

Keyword Categories	**Keyword**
Browser	Google, firefox,
Software	pCloud, pcloud.com
Pictures uploaded	Picturetesting1, Picturetesting2, Picturetesting3, Picturetesting4
PDF uploaded	Example_of_An_Expert_Witness_Digital_for.pdf
Documents	INVESTIGATOR.doc
Password	xcey, testings

The analysis of the four uploaded VMs shows that the pCloud client software was installed in the "C:\Program Files (x86)\" folder. The pCloud sample files and folders were observed on the hard drive, specifically at the default pCloud folder located at "C:\Users\ [username]\pCloud Drive". A drive named "pCloud Drive (P:)" appeared under My Computer. The default pCloud drive comes with five folders (My Music, My Pictures, My Videos, pCloud Help and pCloud Sync), and the details of each file in the folder are summarized in TABLE 7.

TABLE 7 − *Summary of default files that comes with the pCloud client software installation*

Folders	**Name of Files**	**Types of Files**
My Music	Demo Audio 2 GotJoy Lovely Day Momentum	MP3 format sound MP3 format sound Wave sound MP3 format sound
My Pictures	Friends, happy-family, in-the-sky, lovers, romance, sweet	All in JPEG format
My Videos	Pcloud	MP4 video
pCloud help	Getting started with pCloud.pdf	PDF files
pCloud Sync	No files	

The files shown above were analyzed using Access Data FTK Toolkit. This method allows forensic examiners to identify the specific files necessary for an investigation process. The timestamps created by the files stated above,

such as date created, date modified and date of last access, can help examiners determine when a software was last accessed, created in the system or last modified. For example, the last date a file was accessed allows examiners to know the files tampered by criminals. After obtaining this information, examiners can create a storyline of how a crime occurred and obtain crucial information related to a crime. The pCloud drive will be synchronized with the files contained in the hard drives. The synchronization of files in the pCloud Drive with the files in web browsing allows examiners to obtain crucial data and important evidences regarding their investigations.

According to McClain (2011), a Dropbox client software running in a Windows Operating System has a file named "filecache.db", which stores a history of filenames synchronized with Dropbox. These files contain various information. However, "data.db" does not exist in the Dropbox client software (version 1.2.52). Instead, a file with a DBX extension (filecache.dbx) exists, which is encrypted and cannot be interpreted. Studies that analyzed Google Drive also show that "sync_config.db" and "snapshot.db" files exist, which contain the information and downloaded and synchronized files, as well as the details of files associated with cloud storage. Thus, the pCloud analysis shows that a "data.db" file exists in the "C:\Users\ [username]\AppData\Local\pCloud" folder. The "data.db" file holds numerous information, which includes the local path of the pCloud sync and web browsing information used to access pCloud with a number of ports. By determining the location of sync files being stored, examiners can access the content stored in a particular pCloud account without logging in as users.

"data.db" files from pCloud also contain information regarding the metadata of the files stored in the cloud itself. This information includes the parent folder id, hash value of the files, name of the files, type of files, as well as the date of file creation and last modification. Moreover, "data.db" contains crucial information on cloud storage, such as the pCloud client software username and the password associated with the account created. These information aids examiners during evidence acquisition and retrieval, which are normally tedious. For example, a forensic copy of hard drive images obtained from a seized computer hard drive can be run in a related software for data retrieval and scanning. However, information of a pCloud user, such as usernames and passwords stored within ta hard drive, can be exploited easily by criminals who gain remote access to a victim's computer. TABLE 8 presents a summary of the files found in VM hard drives after the analysis of the pCloud client software.

TABLE 8 − *Summary of files found in VMs*

No	Files name	File Location	Description
1	pCloud_Windows.exe	"C:\Users\ [username]\Downloads\" folder	pCloud client software installation files

2	pCloud client software installed	"C:\Program Files (x86)\" folder	pCloud client software installed
3	"data.db"	"C:\Users\ [username]\AppData\Local\pCloud"	Local path of pCloud sync and web browsing information used to access pCloud with the number of port, username, files stored, metadata of the files stored in the cloud itself

Directory Listing of VM hard drives

During testing, a directory listing was produced for each VM created using Access Data FTK Imager Version 3.4.2.6. All the filenames can be viewed using this software. Keyword searches were conducted across the forensic image files created from each VM to filter out a specific keyword of the files in the hard drive. The analysis of the four base VMs created as a control for this test shows that files associated with pCloud sample files, as well as the files stored in a pCloud account before the installation of a pCloud client software , did not exist. Moreover, other uploaded .jpg files, as well as the pdf and document files synced with the pCloud account, did not exist before the client software installation.

Various subsequent filenames associated with pCloud exist in other created VMs, particularly in Upload-, Access-, Uninstall-, Download- Eraser-, and CCleaner-VMs. The files were mostly contained in a folder, such as User's Desktop, Download folders, pCloud Drive (P:\), as well as in the pCloud folder in the hard drive path of "C:\Users\ [username]\pCloud Drive". In upload-VMs, the downloaded installation files "pCloud_Windows_3.3.1" existed in the "C:\Users\ [username]\Downloads\" folder. Access-VMs also retained files associated with pCloud in "data.db".

The timestamps of "data.db" change according to the last time the pCloud client software was ran. Traces of the files uploaded to the pCloud in the pCloud Drive appeared, as shown in TABLE 8. These traces existed because the uploaded files and pictures via web browsing are synced with the pCloud client software and stored in the pCloud Drive (P:\) in the computer hard drive. In Download-VMs, the downloaded files were seen in "C:\Users\ [username]\Downloads\"

The filenames seen after accessing a pCloud account using a web browser were similar with the filenames observed when accessing a pCloud account via a client software because the file was synced with the user's computer local folder C:\Users\ [username] \Documents \ pCloud Sync and also pCloud Drive folder "/pCloud Sync". Finally, the analysis of Eraser-VMs and CCleaner VMs showed that the filenames of deleted files completely vanished from the pCloud sync folder in the user's hard drive. However, the downloaded filenames still existed in the "C:\Users\ [username]\Downloads\" folder until the files were manually deleted from the folder. The deleted

filenames remained in the recycle bin until the user removes them from the recycle bin of the hard drive. Even if the files were cleared from the recycle bin, these can still be retrieved using AccessData FTK imager easily. All the information found through all the files in a computer hard drive help forensic investigators in data analysis. TABLE 9 presents a summary of a directory listing in VM hard drives.

TABLE 9 − *Summary of directory listing in VMs hard drives*

No	VMs	File Names	Location of the files
1.	upload-VMs	pCloud_Windows_3.3.1	C:\Users\ [username]\Downloads\
2	Access-VMs	data.db synced files Synced files	C:\Users\ [username]\AppData\Local\pCloud" pCloud Drive folder "/pCloud Sync" folder C:\Users\ [username] \Documents \ pCloud Sync
3	Download-VMS	Downloaded files	pCloud Drive (P:\) C:\Users\ [username]\Downloads\
4	CCleaner-VMs	Deleted files (picturetesting1.jpg and picturetesting4.jpg)	C:\Users\ [username]\Downloads\
5.	Eraser-VMs	Deleted Files (picturetesting1.jpg and picturetesting4.jpg)	C:\Users\ [username]\Downloads\

Link Files of VMs

The analysis of link files showed that filenames with the extension of .link associated with a pCloud sample, files such as picturetesting3.lnk and picturetesting2.lnk, were located at *"C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent Items"*
in all Upload, Download, Eraser, and CCleaner-VMs. However, other link files were not found within the four Access-VMs. This result indicated that the link files were only created after the files were downloaded and opened. TABLE 10 shows a summary of the link files in the VM hard drives.

TABLE 10 − *Summary of the link files in VM hard drives*

No	Files Names	File Location
1.	picturetesting3.lnk picturetesting2.lnk	"C:\Users\ [username]\AppData\Roaming\Microsoft\Windows\Recent Items

Prefetch files created on VMs after each running the application

Prefetch files can aid forensic investigators in analyzing the applications running on a system. Prefetch files are normally created by Windows when an application is run for the first time from a location to speed up the loading time of applications. Thus, these files contained crucial data on the history of a user's application. For example, CCleaner was run before deleting files and uninstalling the pCloud client software from the hard drive. Moreover, prefetch files still existed in the system even if the client software was uninstalled. Prefetch files were located at "C:\Windows\Prefetch". The prefetch files were viewed using WinPrefetchView v1.35.

Analysis of event logs files

In the current study, event logs were viewed and analyzed by using the built-in Windows event viewer. All the files shown in the event viewer were viewed for all the events that occurred in the VMs throughout the testing time frame. A rule was added to the Windows Firewall exception list when the pCloud client software was installed. Moreover, another rule called "Windows Communication Foundation Net.TCP Listener Adapter (TCP-In)" was also added to the Windows Firewall exception list after the installation of the Microsoft.NET, which was compulsory to install the pCloud client software. Each software installation process was stored when log files "Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx" existed in the "%SystemRoot%\system32\winevt\logs" folder.

Analysis of VM cache files

During the test, the VMware used the stored information regarding guest applications in a directory called caches under the directory where the .vmdk file of each VMs resided. By analyzing the cache directory, a forensic examiner may recover important information, such as the names of files and shortcuts present in a user's desktop, the timestamps of a shortcut being created, its icon, and the timestamps of the application ran for the first time. The ubiquity of virtualization presented ample opportunities for examiners to find useful artifacts in the cache directory of a user's hard drive. Users basically install VMware Tools before the desktop is made available to them for the first time. During the installation of VMware Tools, <VMHome>\caches were created on the host.

PC\Documents\VirtualMachines\caches\<VMHome>\Caches\GuestAppsCache\appdata contains 171 files, which are individually named with a long hex value and the extension .appicon or .appinfo. The file contains the path to the pCloud client application and additional information. Opening the sister file

7e93b9a9e3360c8dc1663ff72f094bab.appinfo in a hex editor shows the installation process of the pCloud client software into the hard drive. This result indicated that a user installed the pCloud software before, and important evidences may be located in a pCloud account. When a user opens an application within the context of a guest VM, there was no change to either of the .appinfo or .appicon pair of files, and the contents of <VMHome>\caches\GuestAppsCache were untouched. The content of the files remained as long as the VM was still used. TABLE 11 presents a summary of VM cache files in the VM hard drives.

TABLE 11 − *Summary of VM cache files in VMs*

No	Files Name	Location of the files
1.	Installation files of VMs	<VMHome>\caches
2.	.appicon or .appinfo files	ThisPC\Documents\VirtualMachines\caches\<VMHome>\Caches\GuestAppsCache\appdata

RAM Analysis

In the current study, VMEM files from the memory were collected in each scenario before the VMs were shut down using AccessData FTK Imager. The analysis of each VMEM files collected from each scenario showed that the term "pCloud" was seen in the VMEM files collected in all scenarios except the Base-VMs. The website URL (www.pcloud.com) was located in all other VMEM files except the Base-VMs.

pCloud account information, such as usernames, was found in the Upload-, Access-, and Download-VMs. Usernames were often found around several texts, which include ">=r....[username]","5username[username]" and also &username=[username]. The passwords of a pCloud account were clearly shown in plaintext around the text "&password=[password] and "*eà [password]". This text can help forensic investigators in running keyword searches to identify the potential pCloud account information of a criminal. Furthermore, data carving was retrieved in thumbnail pictures, as well as partial picture files, recovered from the pCloud sample files in the VMEM files for access, upload, and Download-VMs.

Thumbcache files

Thumbcache files are databases that store thumbnail images of various contents on a system. These databases mentioned are native to Windows Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10 systems. For

example, a thumbnail preview of an image is generated when a mouse is hovered over an image in a folder. The presence of pictures in a Windows thumbnail database is considered an indicator of guilt because a folder containing the pictures must have been opened and viewed through Windows Explorer in a thumbnail; thus, a thumbnail database existed. This existence implied that the user accessed the specific files. In the current study, the analysis of thumbcache files for the four Base-VMs was conducted, and the result showed that pCloud sample pictures did not exist before the pCloud client software was installed and accessed. Moreover, the stored pCloud sample pictures were not found in the Access- or CCleaner-VMs. However, thumbnail samples regarding of the stored pCloud sample files were found in the other VMs, including Upload-, Download-, and Eraser-VMs. Hence, thumbnail images were only stored in the thumbcache files after certain files were downloaded, accessed, or uploaded into an account.

Network PCAP files

In the current study, PCAP files were created using Wireshark and Network Miner 2.0 during the live network capture when pCloud was accessed using different browsers. PCAP files were created to help forensic investigators analyze data network and packet sniffing characteristics. Examining network capture files aids examiners extract information regarding network activities, as well as file remnants associated with pCloud activities. Network traffic was basically observed using Port 80, which was http, and then Port 443, which was https. The analysis showed that when a pCloud account was accessed by either using a client software or a web browser; the analysis showed that a session with IP ranging from 74.120.8.0 to 74.120.8.255 was registered under pCloud.com from Fort Lauderdale, Florida, in the United States. Another session with IP ranging from 54.192.72.0 to 54.192.72.255 was found on Port 80 then to Port 443, which was registered for cloudfront.net located at Woodbridge, New Jersey, United States. Sessions with IP 216.58.221.0- 216.58.221.225 were registered under www.google-anaytics.com from source port TCP 443. TABLE 12 presents a summary of the observed IP lists and their organization from the PCAP file captures.

TABLE 12 − *Summary of observed IP lists and their organization from the PCAP files captured*

IP Address	**Registered Organization**
74.120.8.0-74.120.8.255	My.pCloud.com
216.58.0.0-216.58.0.255	Google Service
54.192.72.0-54.192.72.255	Cloudfront.net
74.125.68.0-74.125.68.255	Stats.doubleclick.net
74.125.200.0-74.125.200.255	www.google.com
54.84.248.0-54.84.248.255	Amazon Web Service
54.210.220.0-54.210.220.255	

Anti-forensic Technique and uninstallation of a pCloud client software

During testing, CCleaner and Eraser were both ran within the computer hard drive to delete the downloaded files from a pCloud account and to uninstall the pCloud client software. However, several data remnants associated with pCloud, such as pCLoud sync files, pCloud cache files and web- browsing history, were still found within the hard drives although the client software was uninstalled. This result indicated that applying anti-forensic toolkits, such as CCleaner and Eraser, cannot completely remove all the traces of the files associated with pCloud. This information can be helpful for forensic investigators to acquire evidences from a user's hard drives.

Thus, the analysis of the data and file remnants shows that only the files installed within the "C:\Program Files (x86)\" folder and pCloud sample files and folders existed in the hard drive. However, the pCloud folder located at "C:\Users\ [username]\pCloud Drive" was deleted. The pCloud Sync folder located at "C:\Users\ [username] \Documents \ pCloud Sync" can still be found in the computer hard drive. All the client software caches and "data.db" that contain the most crucial information regarding the account information still existed in the "C:\Users\ [username]\AppData\Local\pCloud" folder. This outcome showed that numerous file remnants were unaffected after uninstalling the pCloud client software. TABLE 13 shows the summary of files found in the VM hard drives after the uninstallation of the pCloud client software and the files associated with it.

TABLE 13 − *Summary of the files found in VM hard drives after the uninstallation of pCloud client software and the files associated with it*

No	Name of files	Location of files
1	pCloud sample files deleted	C:\Program Files (x86)\
2	pCloud sync folder	C:\Users\ [username] \Documents \ pCloud Sync
3	data.db	C:\Users\ [username]\AppData\Local\pCloud folder.

Presentation of Evidences

A number of data remnant types were found in the hard drives of the VMs after users accessed, downloaded or stored files in the pCloud account. All the obtained evidences aided forensic investigators during case investigations. The current study enables forensic investigators to find a specific file location, which is the source of all the evidences needed in the investigation. By determining the location of evidences, forensic investigators can retrieve the evidences, thereby reducing the time needed to solve a case.

Thus, the analysis of the pCloud client software indicates that information, such as pCloud usernames, passwords, sessionsID, network traffic, prefetch file listing, link files and browsing history, were proven as definitive clues to identify the content of the files that may be crucial to solve a case. The analysis of volatile data was proven effective and conclusive in determining pCloud account access, as well as the networking devices used to connect to the pCloud account, because the devices used to access and synchronize with the pCloud account were shown when a client accessed the account via browsers. This finding is important because each device synchronized with the pCloud account will potentially contain evidences associated with cases investigated. A summary of the analysis results is shown TABLE 14. The tests and implementation processes in finding the location and the data remnants on a user's computer prior to the usage of a cloud storage application for a new cloud storage were conducted successfully. Quick and Choo (7), who used Dropbox as their case study, did not include the information regarding the analysis of VM Cache files, which was proven beneficial in obtaining information regarding the history of files previously ran on a user's computer.

TABLE 14 − *Summary of the analysis findings*

Type of VMs	**Data Remnant Found**				
	Password	**Username**	**Software**	**Sample files**	**Keyword search term**
Base VMs	Nil	Nil	Nil	Nil	Nil
Upload-VMs	Found in RAM	Found in RAM	PCloud_Windows.exe was found after being downloaded. The location of client software installation and the pCloud sample files uploaded were found.	Files were found in prefetch files and link files, among others.	Multiple matches of keyword search obtained
Access-VMs	Found in RAM	Found in RAM	Nil	The information of pCloud software accessed was found residing in cookie, browsing history, pagefiles, and unallocated spaces.	Multiple matches of keyword search obtained
Download-VMs	Found in RAM	Found in RAM	Nil	The downloaded files were stored in the VM hard drives.	Multiple matches of keyword search obtained

Eraser-VMs	Nil	Nil	Nil	The information of pCloud software accessed were found residing in cookie, browsing history, pagefiles, and unallocated spaces. The deleted files were still found in unallocated spaces.	Multiple matches of keyword search obtained
CCleaner-VMs	Nil	Nil	Nil	The information of pCloud software accessed were found residing in cookie, browsing history, pagefiles, and unallocated spaces. The deleted files were still found in unallocated spaces.	Multiple matches of keyword search obtained

Comparison of the Results Taken From Previous Research

Moreover, the directory listing of pCloud showed that synced files identical to the files found in pCloud accounts existed, which helped forensic investigators obtain evidences offline. The analysis of a client software in the present study showed that more information can be found in the "data.db" files created by pCloud than that in the "filecache.dbx" or "host.db" files created by Dropbox. The files "data.db" from pCLoud contained information regarding the local path of pCloud sync and web browsing information used to access pCloud with the number of ports used to access it. However, "filecache.db" and "host.db" only contained information regarding a history of filenames synchronized with Dropbox.

Conclusion and Future Works

With the advancement of the technology era, cloud computing or cloud storage services are gaining acceptance and popularity because of the convenience of using these technologies However, cloud technology poses challenges for forensic practitioners who deal with cybercrimes. Cybercrimes are broad in scope and are defined as attacks that involve the use of computers or networks to commit crimes (3). Data can be uploaded and accessed from different devices without retaining traceable evidences. Thus, determining the types of cloud service providers used by criminals and the user details necessary is crucial for investigations. This information will help forensic investigators identify the location of crucial data and extract and preserve these data in a forensically sound manner. By using pCloud as a case study, we found that the potential data remnant on a Windows 7 computer can be retrieved from the browser history when web access was conducted using different browsers. Client software files, prefetching files, link files, network traffic capture, and memory captures were identified successfully based from the usage of pCloud

for each user activity. Future research may employ experiments regarding mobile devices and examine other newly developed cloud storage services using the same methodology as that in the current study.

Future work of this study will be conducted further by focusing on implementation. An experiment will be conducted to test and evaluate the efficiency of the proposed scheme in locating and collecting artifacts and evidence on cloud computing.

References

1. Hashizume, K., Rosado, D.G., Fernandez-Medina, E., & Fernandez, E.B. An analysis of security issues with cloud computing. Journal of Internet Services and Applications, 2013;4(5):1-13.
2. Federal Bureau of Investigation, Regional Computer Forensics Laboratory, Annual Report for Fiscal Year 2007, Washington, 2017. Retrieved from www .rcfl.gov/downloads/documents/RCFL Nat Annual07.pdf.(Last assessed May 3, 2016).
3. Ahmed, A. A., & Zaman, N. A. K. Attack Intention Recognition: A Review. International Journal of Network Security, 2017;19(2):244-250.
4. Messmer, E. Cloud forensics: In a lawsuit, can your cloud provider get key evidence you need? Network World, March 6, 2013. Retrieved from http://www.networkworld.com/news/2013/030613-cloud-forensics-267447.html. (Last assessed May 7, 2016).
5. D. Reilly, C. Wren, T. Berry. Cloud computing: pros and cons for computer forensic investigations. International Journal of Multimedia and Image Processing, March 2011;1(1): 26–34.
6. M. Taylor, J. Haggerty, D. Gresty, D. Lamb. Forensic investigation of cloud computing systems. Network Security, 2011;2011(3), 4–10
7. Darren Quick, Kim-Kwang Raymond Choo, Dropbox analysis: Data remnants on user machines, Digital Investigation, June 2013;10(1):3-18, ISSN 1742-2876.
8. USDoD. Dod 5220.22-M-Sup 1.National Industrial Security Program Operating Manual Supplement (1995). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/522022Msup1.pdf. (Last assessed June 9, 2016).
9. Ahmed, A. A., Sadiq, A. S., & Zolkipli, M. F. Traceback model for identifying sources of distributed attacks in real time. *Security and Communication Networks*. 2016;9(13):2173-2185.
10. Josiah Dykstra, Alan T. Sherman, Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, Digital Investigation, August 2012; 9(Suppl):S90-S98, ISSN 1742-2876.

11. Hyunji Chung, Jungheum Park, Sangjin Lee, Cheulhoon Kang, Digital forensic investigation of cloud storage services, Digital Investigation, November 2012, 9(2):81-95, ISSN 1742-2876.
12. Kurt Oestreicher, A forensically robust method for acquisition of iCloud data, Digital Investigation, 2014;11(2 Suppl): S106-S113.