Investigating Storage as a Service Cloud Platform: pCloud as a Case Study

Tooska Dargahi\(^a\), Ali Dehghantanha\(^b\), and Mauro Conti\(^c\)

\(^a\)Department of Computer Engineering, West Tehran Branch, Islamic Azad University, Iran;
\(^b\)The School of Computing, Science & Engineering, University of Salford, United Kingdom;
\(^c\)Department of Mathematics, University of Padua, Italy

Abstract

Due to the flexibility, affordability and portability of cloud storage, individuals and companies envisage the cloud storage as one of the preferred storage media nowadays. This attracts the eyes of cyber criminals, since much valuable information such as user credentials, and private customer records are stored in the cloud. There are many ways for criminals to compromise cloud services; ranging from non-technical attack methods, such as social engineering, to deploying advanced malwares. Therefore, it is vital for cyber forensics examiners to be equipped and informed about best methods for investigation of different cloud platforms. In this chapter, using pCloud (an extensively used online cloud storage service) as a case study, and we elaborate on different kinds of artefacts retrievable during a forensics examination. We carried out our experiments on four different virtual machines running four popular operating systems: a 64 bit Windows 8, Ubuntu 14.04.1 LTS, Android 4.4.2, and iOS 8.1. Moreover, we examined cloud remnants of two different web browsers: Internet Explorer and Google Chrome on Windows. We believe that our study would promote awareness among digital forensic examiners on how to conduct cloud storage forensics examination.

Keywords: Cloud Forensics, Computer Forensics, Mobile Forensics, pCloud

This is authors accepted copy, for final version please refer to DOI: 10.1016/B978-0-12-805303-4.00012-5
1. Introduction

The usage of cloud storage, among individuals and companies, is increasing day by day. Due to the recent report of the Forbes (2015), “47% of marketing departments will have at least 60% of their applications on a cloud platform by 2017” [1], and “cloud market cap will pass $500 billion by 2020” [2]. Even though cloud storage offers several advantages compared to traditional and local storage of data, cloud users are concerned about the integrity of stored data, security and user privacy issues [3, 4]. There exist several solutions which could be considered by security experts in order to protect the stored data, and preserve privacy of the cloud users [5, 6, 7, 8]. Adopting security mechanisms is useful in protecting data against being modified and accessed by unauthorized users, and make it difficult for the attackers to abuse the data. However, the artefacts which potentially remain on the cloud storage servers could threaten privacy of the cloud users. In such a case, security mechanisms might not suffice to preserve users’ privacy. As a result, protecting the sensitive data against cloud storage services, which leak the privacy of the users, is trending as an issue to the law enforcement agencies and other digital forensic investigators. Moreover, it should be contemplated that organized cyber criminals are always able to find new ways of evading the rules [9, 10]. This motivated several researchers to conduct a number of cloud storage forensic investigations on various cloud services and applications (apps) [11, 12]. However, with the ever increasing introduction of such cloud services and technologies, having an up to date understanding of possible data remnants after using new cloud storage applications is fundamental for forensic practitioner [13].

In this chapter, we consider pCloud® as a case study to identify the possible evidential data that may remain after the use of pCloud on several different computer systems. pCloud is a free online cloud storage service (founded in 2013 in Switzerland), which has over four million users right today [14]. pCloud users

[1]https://www.pcloud.com/
are able to store, sync and share their files, as well as make backup from other cloud services such as Dropbox. pCloud provides client-side encryption such that the data, which are leaving the client’s system, are encrypted. Moreover, pCloud has the Quality Management Systems (ISO 9001:2008) and Information Security Management Systems (ISO 27001:2013) certificates. Due to the increasing use of the pCloud, and several good reviews that it received from the cloud expert reviewers [15, 16, 17], we are focusing on probable privacy issues of pCloud in this chapter. To the best of our knowledge, this is the first forensics investigative study of pCloud. In particular, We will answer the following questions in the rest of the chapter:

- What data (and the location of the data) can be found on Windows, Ubuntu, Android, and iOS operating systems when using pCloud services?
- What data can be leaked while accessing the pCloud using Google Chrome and Internet Explorer browsers on Windows operating systems?
- What data of forensic interest can be discovered in live memory on the aforementioned platforms?
- What data can be captured from network traffic?

Before introducing our research methodology and contribution of the chapter, we provide a brief literature review on forensic investigation of cloud storage services.

1.1. Related Work

Computer system users produce a great deal of digital data day by day in such a way that by 2020, the amount of produced data will exceed 40 zettabytes [18]. Therefore, in order to store such a data on cloud, we need to have more fast and secure synchronization between servers and PCs; for which services such as BitTorrent are very common these days. In [19], Farina et al. conducted a forensic investigation on the BTSync client application, and recognized the digital artefacts and network findings which could be then
used by digital forensic examiners as an evidence. Due to the increasing use of cloud computing and cloud storage services, researchers believe that cloud computing is more vulnerable to security and privacy issues, such as information theft [20, 21, 22, 23], in particular considering online cloud services [24]. Thus, there is a surge of interest by forensic professionals and privacy experts in cloud forensic analysis in recent years. In this section, we briefly review the state-of-the-art in digital forensics investigation of cloud privacy.

Compared to the other aspects of computer analysis, only a few research studies have been conducted on cloud storage privacy investigation. Martini and Choo [25] were the first to carry out the cloud forensics investigation. They analyzed the ownCloud as a case study, in order to find client and server side artefacts that could be useful as evidential data for forensics practitioners in performing cloud analysis. With the gradual increase of Cloud storage services, there is a growing tendency among individuals and organizations in using such a service in order to store and access several different kinds of data. Therefore, most of the investigations on cloud context are concentrated on analyzing the privacy leakage probability of the widely used cloud storage services. For example, Quick and Choo analyzed the process of gathering data, browsing of data and synchronization of files focusing on Dropbox [26], Microsoft SkyDrive [27], and Google Drive [28]. In [27], the authors found the terrestrial artefacts which are left behind when using SkyDrive on different devices such as mobile phones and desktop computers. Similarly, Quick and Choo studied the possible data remnants on a Windows 7 computer and an Apple iPhone 3G when a user adopts Dropbox [26] or Google Drive [28] in order to store, upload, and access data in the cloud.

Along the same line of study, Hale [29] analyzed the digital artefacts remnant on a computer after accessing or manipulating Amazon Cloud Drive. They could recover several information, such as installation path, and upload/download operations. In [30], Chung et al. presented new method in order to analyze the digital artefacts left on all accessible devices, such as Mobile phones (e.g., iPhone and Android smartphone) and Desktop systems, running different OS
(e.g., Windows and Mac) while using Amazon S3, Google Docs, Dropbox, and Evernote. Contrary to most of the cloud storage services that are based on open source platforms, Apple users, have their own special cloud storage called iCloud. Östreicher [31] investigated particularly iCloud service in order to find leftover digital droplets when using native Mac OS X during system synchronization with the cloud. There are also various research studies on several different cloud storage services that we summarized in Table 1. We refer the interested reader to [32, 33] for a comprehensive survey in this regard.

Table 1: A brief overview of the existing cloud storage forensics research studies.

| Cloud Services       | Public Cloud | Private Cloud |
|----------------------|--------------|---------------|
| Dropbox              | [30, 34, 35, 36, 36, 12, 37] | [35]          |
| Amazon S3            | [30]         |               |
| Evernote             | [30]         |               |
| Google Drive         | [30, 34, 38, 38, 12, 37] |               |
| SkyDrive             | [34, 37, 12] |               |
| Box                  | [35, 37]     | [35]          |
| SugarSync            | [35, 39]     | [35]          |
| Amazon Cloud Drive   | [29]         |               |
| OneDrive             | [36, 37]     |               |
| ownCloud             | [26]         | [25]          |
| Flicker              | [48]         |               |
| PicasaWeb            | [38]         |               |
| iCloud               | [31]         |               |
| UbuntuOne            | [40]         |               |
| hubiC                | [41]         |               |
| Mega                 | [42]         |               |
| Hadoop               | [43]         |               |
| Amazon EC2           | [44]         |               |
| vCloud               | [45]         |               |
| XtreemFS             | [46]         |               |
| Eucalyptus           | [47]         |               |
| Amazon AWS           | [48]         |               |

Outline. The rest of the chapter is organized as follows: in Section 2 we explain the research methodology and experimental setup. Section 3 presents the results of our experimental analysis on pCloud. We answer the question “What data can be captured from network traffic?” in Section 4. Finally, Section 5 concludes the chapter.
2. Research Methodology

In order to conduct a reliable digital forensic analysis, we should follow a forensic investigation guideline [49, 50]. In this research study, we performed our forensic investigation based on the framework introduced by Martini and Choo [51] which is composed of four important stages (Figure 1):

![Cloud forensics framework of Martini and Choo [51]](image)

- **Evidence source identification and preservation.** In this phase, we detect potential sources of evidences. We used *VMware Workstation 10.0.2 build 1744117* to create the Virtual Machines (VMs) for the experiments. We configured each virtual machine with 1 GB of RAM, and 2 GB hard disk space for Android VM, 15 GB for Ubuntu VM, and 40 GB Windows VM.

- **Collection.** In this phase, we collected the potential data resources and files in a forensically sound manner.

- **Analysis.** In this phase, we analyzed the data obtained from the previous phase. We considered keywords such as “account”, “password”, and “files” to search for evidence in the memory. This chapter is mainly focused on presenting analysis results of pCloud platform, however, we highlighted the collection and preservation approaches as deemed necessary!
- **Reporting and presentation.** This phase presents the collected evidences, in such a way that would be acceptable by the court of law. As this chapter is only focused on presenting potential evidences; we just shortly discussed this stage in conclusion.

2.1. Experimental Setup

We conducted our experiments on four different operating systems: a 64 bit Windows 8, Ubuntu 14.04.1 LTS, Android 4.4.2, and iOS 8.1. We considered two different browsers: **Internet Explorer 10.0.9200.16384** and **Google Chrome 39.0.2171.71 m**. We carried out our experiments using the digital forensic research workshop challenge 2013 dataset (DFRWS\(^2\)). We downloaded the dataset on 08\(^{th}\) December 2014 and evaluated the hash of the dataset to ensure the integrity of the data. The dataset contains a main folder called **test** including ten directories namely: au, b, img, js, ml, msx, pdf, txt, vid, z. We carried out our investigation taking into account all the files included in all directories.

We utilized **Wireshark 1.12.3** to capture network traffic in all of the platforms and experimental tasks running on them. Furthermore, we used **NetworkMiner 1.6.1** to further analyze the captured network traffic. We captured physical memory in Ubuntu using **memdump 1.01-6-i386**. We used **Hex Workshop 6.7** (6.8.0.5419 / 1\(^{st}\) Sep. 2014) to analyze the captured physical memory of the virtual machines, after the successful execution of each task. One of the main goals of examining this type of application is to determine the possible remnants on different platforms using certain tools, which we explain in the following. Apart from the **sqlitebrowser 3.4.0**, we also adopted **iphonebackupbrowser-r38** for Android and iOS.

2.1.1. Windows

In order to investigate pCloud remnants on a Windows operating system, we considered two different research directions: i) Windows web browser-based

\(^2\)http://www.dfrws.org/2013/challenge/index.shtml
analysis, and ii) Windows application-based analysis.

As for the web browser-based investigation, we installed two popular browsers: Microsoft Internet Explorer 10.0.9200.16384, and Google Chrome 39.0.2171.71 m on four VMs, and performed different tasks specifically to the VM. Figure 2 shows the web browser-based tasks on the Windows VM. We updated Microsoft Internet Explorer, and installed Google Chrome on the base machine. We then cloned to four other machines for the following tasks: upload, download, open and delete. Since it is a browser-based experiment, installation of pCloud was not required, as the experiment will be directly focusing on interacting with the pCloud in the web browser. We used all the folders and files from the DFRWS dataset during each task. For example, we first uploaded all the files during the upload task, and then downloaded back during the download task. Moreover, we captured network traffic during all the tasks.

![Figure 2: Windows browser-based VMs.](image)

The main artefacts which are recoverable from web browsers are from their cache and history folders. Therefore, after performing the four aforementioned operations (i.e., upload, download, open and delete) using the dataset, we analyzed the cache using **NirSoft IECacheView v 1.53** for Internet Explorer and **NirSoft ChromeCacheView v 1.61** for Google Chrome.

In order to conduct the windows app-based investigation, we adopted Windows 8.1 Pro build 9600 with pCloud drive 2.0. We performed six different tasks as it can be seen in Figure 3.
2.1.2. Android

In order to access the system folders on Android, the OS needs to be rooted. Without the root access, there is no way of accessing the data which are required to perform the experiments and capturing the internal memory. Also having the root access, we will be able to run certain commands and access system protected files. To interact with the given Android machine, we used a terminal called Android emulator 1.0.5. We accessed the system protected files using an application called Root Browser 2.2.3. With the help of this file browser, we were able to locate different critical artefacts related to the pCloud, such as databases and log files. We used terminal emulator in order to capture the processes which were running in the internal memory (RAM Capture) and also to copy the captured file to the main investigation machine. We carried out six different experiments on Android based application (Android 4.4.2), which are depicted in Figure 3.

2.1.3. iOS

In order to conduct experiments on iOS, we adopted an iPad mini running iOS 8.1. However due to some authentication issues from the owner, we were unable to jail break. We used iTunes 12.0.1.26, 64 bit, to back up the files after performing the tasks which are shown in Figure 3. After completion of each task, we took a back up of the whole ipad using iTunes with the use of iPhone Backup Browser 1.2.0.6 (by Google project). We were able to track the changes which was made during the installation procedure of the pCloud.
2.1.4. Ubuntu

We adopted the *Ubuntu 14.04.1 LTS* (Trusty Tahr) to carry out our investigation. We installed the pcloud drive 2.0 through the Ubuntu software center. We also performed the uninstallation process through the Ubuntu software center. We installed the pCloud drive on a main VM which was the “install and login”. We also cloned this virtual machine for the other tasks: upload, download, sync, open, delete and uninstallation (see Figure 3). In fact, we cloned these machines in order to avoid the virtual memory being overwritten by the execution of the next task, which would erase the evidence of the previous task with the new evidence of the next task.

The DFRWS dataset contained various types of files, and we used all of them in the experiments. For example, during upload, we uploaded all the folders and files. After the successful execution of each task, we captured the live memory using *memdump 1.01-6*. During carrying out all the tasks, we also captured the network traffic using *Wireshark 1.12.3*.

3. Analysis and Findings

In this section, we present our experimental findings along with the data analysis. In order to analyze the live memory we accessed the VM folders while the VM was powered on. We analyzed this memory, using *Hex Workshop*, after the corresponding task was successfully performed on the VM. It should be noted that, if we do not mention a specific action (such as download, upload, sync, or delete), it means there was no evidence which could be used by a forensic investigator for further analysis of that action.

3.1. Windows Browser-Based Experiments

We first set up the base virtual machine in order to conduct the experiments over Windows browser-based. As all the clones had the latest version of the Internet Explorer and Google Chrome, we avoided installing and updating the browsers when conducting experiments. We started the experiments with the
“upload” VM, leading to the “download” VM, and after that “open” and “delete” VMs.

3.1.1. Upload

We were able to acquire information such as uploaded file names and the user names, which was used to upload the data to the pCloud, using Internet Explorer. As Figure 4 shows, we could discover the folder path from the memory.

![Figure 4: Windows Browser-based – Uploaded Files](image)

3.1.2. Install and Login

As it can be seen in Figure 5, the passwords and the email address are clearly discoverable from the physical memory, along with the interested file names and directories. These information are valuable for a forensic examiner.

![Figure 5: Windows Browser-based – Install and Login](image)

We utilized NirSoft IEPassView 1.32 in order to analyse the saved data files by the Internet Explorer. We found out that Internet Explorer saves the pCloud credentials in the registry. However, search results do not reveal any kind of information regarding the credentials in the Internet Explorer cache files, for which we used IECacheview to perform analysis. Obtained results indicate that all the uploads went through an encrypted server, making it difficult to gather much information about the uploads.
We also analyzed the memory image focusing on the Google Chrome browser. We were able to retrieve remnants such as username and password which was used to access pCloud (Figure 6). We could also find evidential data through ChromeCacheView for Google Chrome cache, along with the links which were accessed during the tasks.

3.2. Windows app-Based Experiments

In this section we discuss the evidential data we obtained while analysing the pCloud application (app) installed on Windows OS. We explain three different tasks: Install and Login, Delete, and Uninstall.

3.2.1. Install and Login

Upon the first installation of the pCloud on Windows, we have traced down the changes that the app made on both file system and the registry of the computer. The pCloud client created and modified the following address on the disk drive: Users\User\Documents\pCloud Sync. This address is used to store the pCloud client files, the configuration and some other necessary files. Other than the system’s disk drive, pCloud has created entries in the registry of the Windows. The Registry entries can be find in the following locations:

- HKEY_CURRENT_USER\Software\pcloud
- HKEY_CURRENT_USER\Software\pcloud LTD\pCloud Drive
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3e0d7412-ce78-4007-a287-f4a4b42460b2}\DisplayName: "pCloud Drive"
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3e0d7412-ce78-4007-a287-f4a4b42460b2\}\DisplayVersion: "2.0.3.0"

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3e0d7412-ce78-4007-a287-f4a4b42460b2\}\Publisher: "pCloud LTD"

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\{9CB654A6-2141-46DA-A953-0FCB19FE13CA\}: "v2.22|Action=Allow|Active=TRUE|Dir=In|Protocol=6|App=% ProgramFiles(x86)%\pCloud\Drive\pCloudDrive.exe|Name=pCloud|Edge=TRUE"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\2CB735048C972D445A5864132F3A0314\InstallProperties\DisplayName: "pCloud Drive"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\2CB735048C972D445A5864132F3A0314\InstallProperties\Publisher: "pCloud LTD"

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3e0d7412-ce78-4007-a287-f4a4b42460b2\}\QuietUninstallString: "%ProgramData%\PackageCache\{3e0d7412-ce78-4007-a287-f4a4b42460b2\}\pCloud Drive.exe /uninstall /quiet"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B8991F4234EFEBC4F8A2180B2B003A2C\2CB735048C972D445A5864132F3A0314: "01:\Software\pCloud\AppPath"

HKLM\SOFTWARE\Classes\CLSID\{0673fac-351f-3948-9d8a-1dad9d870193\}\InprocServer32\CodeBase:file://\%ProgramFiles(x86)%\pCloudDrive/ContextMenuHandler.DLL
We found out that pCloud creates some files in the **Run** and also **Uninstall** folders of the registry. Other than changes in the registry and local hard drive, we noticed changes in the rules for Windows Firewall in order to solve the issues that may happen while connecting to the pCloud Servers (Figure 7).

![Figure 7: Windows app-based registry changes in firewall folder](image)

After reviewing the memory dump images from the Windows machine, which pCloud client was installed on, we found out that we are unable to find any sort of plain text passwords. However, we have successfully found usernames within the memory dump.

### 3.2.2. Delete

In order to analyse the effect of the “Delete” action, we deleted some files. We recognized that it is still possible to find some traces of the deleted file names within the memory dump (Figure 8).

![Figure 8: Windows app-based deleted files](image)

### 3.2.3. Uninstall

After the uninstallation process of the pCloud from the VM, we detected two registry entries (Figure 9).

![Figure 9](image)
Other than the changes in registry, there were some files left on the disk after uninstallation of the application, which were located at: \User\AppData\local\pCloud. Moreover, we found out that pCloud client stores every information such as “account information” and the “files summery” in a database called Data.db on the computer. This database uses sqlite dbms system. From this database file, we were able to extract different kinds of data such as “uploaded file names”, and “usernames” which the client used to access the pCloud. Moreover, by analysing the database, we found a table called “file” which keeps all the stored files names. We could find all the files, which we created on our pCloud account. Furthermore, we were able to recover our pCloud account information, such as “userid” and “username” in a table called “settings”.

3.3. Android app-Based Experiments

In this section, we provide our experimental results related to the pCloud application when using Android OS. We considered three tasks: Install and Login, Upload and Uninstall.

3.3.1. Install and Login

Once the pCloud was installed on the Android platform, the following two folders were created:

- /Device/data/data/com.pcloud.pcloud
- /emulated/0/.pcloud/

By using “Root Browser”, it is possible to locate those folders after completion of the installation process. Moreover, an examination of the memory
capture revealed useful information other than user login details, such as folder paths, its database location and other pCloud related information. We recognized that the database for pCloud was stored in the following locations:

- /data/data/com.pcloud.pcloud/databases/PCloudDB/
- /data/data/com.pcloud.pcloud/databases/PCloudDB-journal/

Analysing the database using Sqlitebrowser 3.4.0, it is possible to find “user-names”, “email quota”, and “tables”, which are related to pCloud communications. Once the pCloud was installed, we logged in from the account which we created previously. Then, the system analyser dumped the whole memory of Android and sent it to analysis machine for further analysis. We analyzed the memory using Hex Workshop 6.7. In order to find data related to the user account, we used a search string (i.e., “account=”). This way, we could identify the account which we had registered for the cloud storage (Figure 10).

Figure 10: Android – account details

Upon finding the registered account, we used it in order to check if it is possible to find more credentials' details! Figure 11 shows the extracted artefacts highlighted in yellow.

3.3.2. Upload

Considering the upload task, we could recover some of the files, which were uploaded to the pCloud, from the memory capture. To this end, we used the search string “file”. A part of the files are demonstrated in Figure 12 (the highlighted parts).
3.3.3. Uninstall

In order to investigate the possible evidential data which could be remained on the memory after uninstallation of the application, we uninstalled the pCloud application and captured the memory. We could recover some of the folders which were already created in the installation process. We were also able to recover some of the details by accessing the default browser in Android. We logged into the pCloud service using Android default web browser, then we analyzed the cache file, and browser history. We could recover evidences such as website information, and some cookie files regarding the access of pCloud.

3.4. iOS Based Experiments

Examining iOS for finding possible pCloud artefacts was difficult due to the complexity of the OS, compared to other operating systems. Moreover, we were unable to Jail break iOS. Therefore, we adopted backup investigation method to detect the exact location of the installed pCloud.
Upon installation of the pCloud on iOS, the folders/files which are depicted in Figure 14 were created in the following locations:

- **Library/Preferences/com.pcloud.pcloud.plist**
- **Library/googleanalytics-v2.sql**
- **Library/googleanalytics-v3.sql**
- **Library/Application Support/p.db**

During the analysis process of the iOS backup files, we didn’t find any login details related to pCloud. However, we obtained some information such as “session ID” (type of cookie which the web servers store for a specific user for a duration of time), and “API key” (a code passed to the computer to identify the calling program to its user), which then could be useful for Forensic Investigations (see Figure 15). Furthermore, we could obtain information such as pCloud installation directory location.
3.4.1. Upload and Uninstallation

Even though we did not obtain pCloud login details on iOS, we could detect some useful information such as “uploaded files names” (as highlighted in Figure 16). Moreover, upon uninstallation we could recover some of the deleted files. In order to access such information, we used several search strings such as common file types, for instance “.jpg” and “.pdf”.

Figure 16: iOS based uploaded file names found in the backup files
3.5. Ubuntu app-Based Experiments

During the experimental study on Ubuntu, we installed the pCloud drive 2.0 on base VM, and logged in. Then, we cloned it for several tasks, which we carried out in the following sequential manner: upload, download, sync, open, delete and uninstall. We analyzed all the acquired memory dump files using *hex workshop*. We found quite a number of evidences in the memory. These evidences are clearly useful for digital investigators in order to get to know the “username”, “password”, and “files names” of the victim or suspects.

As it is demonstrated in Figure 17, it is possible to recover the “username” and “password” of the user during installation and login process. These information have high forensic value to the forensic examiners as it shows the credentials of the victims/suspects. Moreover, as Figure 18 shows, we can retrieve the uploaded file names and the file path from the memory dump. We could also retrieve the same evidences as the ones extracted from the “upload VM memory dump, during the sync and download tasks. As it is depicted in Figure 19 after the deletion of the files from the app, it is possible to recover “username” from the memory dump. This evidence can also help the forensic examiners to identify the credentials that were used.

Figure 17: Ubuntu – revealed credentials during install and login tasks.

Figure 18: Ubuntu – extracted information during upload process.

Figure 19: Ubuntu – recovered username after deletion task.
4. Network Traffic

Compared to the evidential data recovered from the storage and memory, we could obtain relatively limited amount of data by analysing the network traffic. This is mostly because pCloud uses encrypted connections, such as TLSv1.2 and HTTPS over SSL certificates, which are then provided by external vendors. During the download and upload tasks, an encrypted connection is established with protocol HTTPS.

In Table 2, we show some relevant IP addresses to pCloud, which we could recover during the Internet Explorer experiment. We can conclude that all the connections to these hosts were over TCP port 443, and used a TLSv1.2 Encryption. Apart from these IP addresses, we were able to track the service providers for SSL certificates, along with the main login IP address/URL which we could use as forensic investigators for further analysis. The recovered SSL Certificate providers list is as follows:

- http://silver-server-g2.ocsp.swisssign.net/
  D3446FD9FE7AFCDEAC1C7AA2210D64FA65B0D782
- http://crl.swisssign.net/D3446FD9FE7AFCDEAC1C7AA2210D64FA65B0D782
- ldap://directory.swisssign.net/
  CN=D3446FD9FE7AFCDEAC1C7AA2210D64FA65B0D782%
  2C0=SwissSign2C0=CH?certificateRevocationList?base?objectClass=cR
  LDistributionPoint

5. Conclusion

In this chapter, by analysing pCloud as a case study we demonstrated the possibility to recover a numerous amount of residual evidences from this platform. We analyzed the pCloud on several operating systems (i.e., Windows, Android, iOS, Ubuntu) considering different tasks (such as, install, login, upload, download, uninstall). We showed that all the pCloud credentials could
be extracted along with the files that were used for storage. Even though the network connections were encrypted, some of the credentials used in almost all platforms were in plain text format which is an added advantage for forensic investigators. However we were only able to collect login credentials by capturing the live memory at the time of installation of the pCloud service. So it is highly recommended for forensic investigators to capture the memory at the time of installation.

Our presented research study in this chapter may pave the way for forensics examiners investigating pCloud and other cloud storage platforms. In future, researchers can use similar investigation method to retrieve other cloud platforms remnants. Extending presented approach for detecting evidences of different platforms over cloud, such as investigating mobile devices connected to the cloud, investigation of cloud-based social networking platforms, and cloud malware forensics would be interesting future works. Moreover, analyzing legal and privacy implications of conducting cloud forensics and developing relevant solutions could further opportunities for real-world utilization of cloud investigation techniques.
Table 2: Recovered IP addresses during the Internet Explorer experiments.

| IP Address | Host Name                  | Activity       |
|------------|----------------------------|----------------|
| 74.120.8.17 | binapi.pcloud.com          | Install and Login |
| 74.120.8.24 | binapi.pcloud.com          | Uninstall      |
| 74.120.8.8  | C47.pcloud.com             |                |
| 74.120.8.26 | binapi.pcloud.com          | Upload         |
| 74.120.8.28 | C1.pcloud.com              |                |
| 74.120.8.41 | C19.pcloud.com             |                |
| 74.120.8.56 | C47.pcloud.com             |                |
| 74.120.8.64 | C54.pcloud.com             |                |
| 74.120.8.73 | C81.pcloud.com             |                |
| 74.120.8.89 | C72.pcloud.com             |                |
| 74.120.8.92 | C75.pcloud.com             |                |
| 74.120.8.96 | C79.pcloud.com             |                |
| 74.120.8.100 | C82.pcloud.com          |                |
| 74.120.8.133 | C94.pcloud.com        |                |
| 74.120.8.77 | a2.pcloud.com, translate.pcloud.com | Upload     |
| 74.120.8.15 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.14 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.14 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.34 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.34 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.15 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.14 | api.pcloud.com, my.pcloud.com |                |
| 74.120.8.34 | api.pcloud.com, my.pcloud.com |                |

References

[1] L. Columbus, Predicting the future of cloud service providers, [http://www.forbes.com/sites/louiscolumbus/2015/04/05/predicting-the-future-of-cloud-service-providers/](http://www.forbes.com/sites/louiscolumbus/2015/04/05/predicting-the-future-of-cloud-service-providers/) (Accessed 27 June 2015) (2015).

[2] A. Konrad, Report: Cloud market cap to pass $500 billion by 2020, [http://www.forbes.com/sites/alexkonrad/2015/06/18/byron-deeter-state-of-the-cloud/](http://www.forbes.com/sites/alexkonrad/2015/06/18/byron-deeter-state-of-the-cloud/) (Accessed 27 June 2015) (2015).

[3] D. Chen, H. Zhao, Data security and privacy protection issues in cloud computing, in: Proceedings of the International Conference on Computer
Science and Electronics Engineering, Vol. 1 of ICCSEE'12, IEEE, 2012, pp. 647–651.

[4] C. A. Ardagna, M. Conti, M. Leone, J. Stefa, An anonymous end-to-end communication protocol for mobile cloud environments, IEEE Transactions on Services Computing 7 (3) (2014) 373–386.

[5] H. Takabi, J. B. Joshi, G.-J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Security & Privacy (6) (2010) 24–31.

[6] A. Mathew, Survey paper on security & privacy issues in cloud storage systems, in: Electrical Engineering Seminar and Special Problems B, Vol. 571, 2012.

[7] S. Hosseinzadeh, S. Hyrynsalmi, M. Conti, V. Lepp, et al., Security and privacy in cloud computing via obfuscation and diversification: A survey, in: Proceedings of the 7th International Conference on Cloud Computing Technology and Science, CloudCom’15, IEEE, 2015, pp. 529–535.

[8] M. R. Memarian, M. Conti, V. Leppanen, EyeCloud: A BotCloud detection system, in: Proceedings of the 5th IEEE International Symposium on Trust and Security in Cloud Computing, Vol. 1 of TSCloud’15, IEEE, 2015, pp. 1067–1072.

[9] K.-K. R. Choo, R. G. Smith, Criminal exploitation of online systems by organised crime groups, Asian Journal of Criminology 3 (1) (2008) 37–59.

[10] K.-K. R. Choo, Organised crime groups in cyberspace: a typology, Trends in organized crime 11 (3) (2008) 270–295.

[11] D. Quick, B. Martini, R. Choo, Cloud storage forensics, Syngress, 2013.

[12] D. Quick, K.-K. R. Choo, Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?, Digital Investigation 10 (3) (2013) 266–277.
[13] F. Daryabar, A. Dehghantanha, N. I. Udzir, et al., A review on impacts of cloud computing on digital forensics, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2 (2) (2013) 77–94.

[14] pcloud, about the company, https://www.pcloud.com/company/about.html (Accessed April 2016).

[15] Cloudswave awards 2015: Introducing the 10 best document management software, http://www.cloudswave.com/blog/cloudswave-awards-2015-introducing-the-10-best-document-management-software/ (Accessed 1 July 2015) (2015).

[16] F. Barton, pcloud drive 3.0: Findmysoft editor’s review, http://pcloud-drive.findmysoft.com/ (Accessed 1 July 2015) (2014).

[17] S. Fisher, pcloud review, http://freebies.about.com/od/computerfreebies/fl/pcloud-review.htm (Accessed 1 July 2015) (2015).

[18] L. Mearian, By 2020, there will be 5,200 gb of data for every person on earth, http://www.computerworld.com/article/2493701/data-center/by-2020-there-will-be-5-200-gb (Accessed 9 July 2015) (2012).

[19] J. Farina, M. Scanlon, M.-T. Kechadi, Bittorrent sync: first impressions and digital forensic implications, Proc. of the First Annual DFRWS Europe Digital Investigation 11 (2014) S77–S86.

[20] K.-K. R. Choo, et al., Cloud computing: challenges and future directions, Trends and Issues in Crime and Criminal Justice (2010) 1–6.

[21] J. Galante, O. Kharif, P. Alpeyev, Sony network breach shows amazon clouds appeal for hackers, http://www.bloomberg.com/news/2011-05-15/sonyattack-shows-amazon-s-cloud-service-lures (Accessed 5 June 2014) (2011).

[22] Symantec, The trojan. hydraq incident: Analysis of the aurora 0-day exploit,
[23] A. Duke, 5 things to know about the celebrity nude photo hacking scandal, http://edition.cnn.com/2014/09/02/showbiz/hacked-nude-photos-five-things/ (Accessed 18 November 2014) (2014).

[24] M. Taylor, J. Haggerty, D. Gresty, D. Lamb, Forensic investigation of cloud computing systems, Network Security 2011 (3) (2011) 4–10.

[25] B. Martini, K.-K. R. Choo, Cloud storage forensics: ownCloud as a case study, Digital Investigation 10 (4) (2013) 287–299.

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

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

[28] D. Quick, K.-K. R. Choo, Google drive: Forensic analysis of data remnants, Journal of Network and Computer Applications 40 (2014) 179–193.

[29] J. S. Hale, Amazon cloud drive forensic analysis, Digital Investigation 10 (3) (2013) 259–265.

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

[31] K. Oestreicher, A forensically robust method for acquisition of icloud data, Digital Investigation 11 (2014) S106–S113.

[32] B. Martini, K.-K. R. Choo, Cloud forensic technical challenges and solutions: a snapshot, IEEE Cloud Computing (4) (2014) 20–25.

[33] A. Pichan, M. Lazarescu, S. T. Soh, Cloud forensics: technical challenges, solutions and comparative analysis, Digital Investigation 13 (2015) 38–57.
[34] C. Federici, Cloud data imager: A unified answer to remote acquisition of cloud storage areas, Digital Investigation 11 (1) (2014) 30–42.

[35] G. Grispos, W. B. Glisson, T. Storer, Using smartphones as a proxy for forensic evidence contained in cloud storage services, in: Proceedings of the 46th Hawaii International Conference on System Sciences, HICSS’13, IEEE, 2013, pp. 4910–4919.

[36] B. Martini, Q. Do, K.-K. R. Choo, Mobile cloud forensics: An analysis of seven popular android apps, arXiv preprint arXiv:1506.05533.

[37] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, K.-K. R. Choo, Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices, Australian Journal of Forensic Sciences (2016) 1–28.

[38] F. Marturana, G. Me, S. Tacconi, A case study on digital forensics in the cloud, in: Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC’12, IEEE, 2012, pp. 111–116.

[39] M. Shariati, A. Dehghantanha, K.-K. R. Choo, Sugarsync forensic analysis, Australian Journal of Forensic Sciences 48 (1) (2016) 95–117.

[40] M. Shariati, A. Dehghantanha, B. Martini, K. Choo, Ubuntu One investigation: Detecting evidences on client machines.

[41] B. Blakeley, C. Cooney, A. Dehghantanha, R. Aspin, Cloud storage forensic: hubiC as a case-study, in: Proceedings of the 7th International Conference on Cloud Computing Technology and Science, CloudCom’15, IEEE, 2015, pp. 536–541.

[42] F. Daryabar, A. Dehghantanha, K.-K. R. Choo, Cloud storage forensics: MEGA as a case study, Australian Journal of Forensic Sciences doi:10.1080/00450618.2016.1153714.
C. Cho, S. Chin, K. S. Chung, Cyber forensic for hadoop based cloud system, International Journal of Security and its Applications 6 (3) (2012) 83–90.

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

B. Martini, K.-K. R. Choo, Remote programmatic vCloud forensics: a six-step collection process and a proof of concept, in: Proceedings of the 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom’14, IEEE, 2014, pp. 935–942.

B. Martini, K.-K. R. Choo, Distributed file system forensics: XtreemFS as a case study, Digital Investigation 11 (4) (2014) 295–313.

F. Anwar, Z. Anwar, et al., Digital forensics for eucalyptus, in: Proceedings of the Frontiers of Information Technology, FIT’11, IEEE, 2011, pp. 110–116.

R. Marty, Cloud application logging for forensics, in: Proceedings of the ACM Symposium on Applied Computing, ACM, 2011, pp. 178–184.

S. Wilkinson, Acpo good practice guide for digital evidence (2011).

K. Kent, S. Chevalier, T. Grance, H. Dang, Guide to integrating forensic techniques into incident response, NIST Special Publication.

B. Martini, K.-K. R. Choo, An integrated conceptual digital forensic framework for cloud computing, Digital Investigation 9 (2) (2012) 71–80.

S. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, Smartphone forensics: a case study with nokia e5-00 mobile phone, International Journal of Digital Information and Wireless Communications (IJDIWC) 1 (3) (2011) 651–655.
[53] S. Parvez, A. Dehghantanha, H. G. Broujerdi, Framework of digital forensics for the samsung star series phone, in: Proceedings of the 3rd International Conference on Electronics Computer Technology, Vol. 2 of ICECT’11, IEEE, 2011, pp. 264–267.

[54] S. Mohtasebi, A. Dehghantanha, Defusing the hazards of social network services, International Journal of Digital Information and Wireless Communications (IJDIC) 1 (2) (2011) 504–515.

[55] F. Norouzizadeh Dezfooli, A. Dehghantanha, B. Eterioric-Soric, K.-K. R. Choo, Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms, Australian Journal of Forensic Sciences (2015) 1–20.

[56] F. Daryabar, A. Dehghantanha, H. G. Broujerdi, Investigation of malware defence and detection techniques, International Journal of Digital Information and Wireless Communications (IJDIC) 1 (3) (2011) 645–650.

[57] F. Daryabar, A. Dehghantanha, N. I. Udzie, Investigation of bypassing malware defences and malware detections, in: Proceedings of the 7th International Conference on Information Assurance and Security, IAS’11, IEEE, 2011, pp. 173–178.

[58] K. Shaerpour, A. Dehghantanha, N. Mahmod, Trends in android malware detection, The Journal of Digital Forensics, Security and Law: JDFSL 8 (3) (2013) 21.

[59] F. N. Dezfooli, A. Dehghantanha, N. Mahmod, N. F. B. M. Sani, S. B. Shamsuddin, F. Daryabar, A survey on malware analysis and detection techniques, International Journal of Advancements in Computing Technology 5 (14) (2013) 42.

[60] M. Damshenas, A. Dehghantanha, R. Mahmoud, A survey on malware propagation, analysis, and detection, International Journal of Cyber Security and Digital Forensics (IJCSD) 2 (4) (2013) 10–29.
[61] F. Daryabar, A. Dehghantanha, N. I. Udzir, M. Sani, S. bin Shamsuddin, F. Norouzizadeh, et al., A survey on privacy impacts of digital investigation., Journal of Next Generation Information Technology 4 (8).

[62] A. Dehghantanha, K. Franke, Privacy-respecting digital investigation, in: Proceedings of the 12th Annual International Conference on Privacy, Security and Trust, PST’14, IEEE, 2014, pp. 129–138.