TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

TUT Center for Digital Forensic and Cyber Security

FORENSIC ANALYSIS OF CLIENT-SIDE ARTIFACTS ON CLOUD BASED APPLICATION

ITC70LT

Prabin Krishna Subedi 165495IVCM

Supervisor

Hayretdin Bahsi

PhD

Tallinn 2019

Authors declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Prabin Krishna Subedi

11.05.19

Abstract

Currently, cloud storage service is widely accepted by business and individuals. This acceptance of use of cloud storage equally valid for cybercriminal as cloud storage service has become calm platform to conduct malicious activity which turns out to be challenge to forensic investigator and researcher. In this research we come up with technical guidelines to identify and collect the forensic evidences from end user machine thus generated while using cloud storage client application to access the remote cloud storage unit for multiple actions like login, upload, download, delete and logout. During this thesis we have developed a technical procedure for forensic investigation for the client machine based on windows 7 OS, cloud storage client application Cyberduck and three popular cloud storage service providers Digital Ocean Spaces, IBM COS and Rackspace cloud files.

We proceed with the gathering the Installation artifacts related Cyberduck client application on windows 7 OS, network analysis, volatile memory analysis and disk analysis. To proceed with all three Cloud, we consider three cases of study which covers all identification and collection of forensic artifacts of our interest thus generated due to user action like login, upload, download, delete and logout based on network, volatile memory and disk analysis as a part of windows forensic. The major evidences identified and collected during this study are remote file metadata, client software installation artifacts, username/password, deleted file metadata on client machine and others regular artifacts that is of forensic interest.

Thus, the procedure developed within this research study will provide a complete guideline to the forensic investigator and researcher during the study of similar kind of case in real world scenario.

List of Abbreviations and Terms

NIST	National Institute of Standards and Technology
MFT	Master File Table
NTFS	New technology File System
CDN	Content Delivery Network
iOS	iPhone Operating System
RAM	Random Access Memory
TLS	Transport Layer Security
GUI	Graphical User Interface
IBM	International Business Machine
COS	Cloud Object Storage
IP	Internet Protocol
VM	Virtual Machine
LAN	Local Area Network
HTTP	Hyper Text Transfer Protocol
API	Application Program Interface

Table of Contents

List of Figures

List of Tables

1. Introduction

Currently, cloud computing can be claimed as a significant part of every IT industry and can be stated as very promising and attractive solutions. It holds several benefits such as on demand service with high availability, reliability and scalability, and flexible pay as you go (low cost), which are much more suitable for small and medium scale industry. Such benefits with cloud computing motivated many businesses to migrate their IT infrastructure to cloud or accept cloud computing as prime technology. As a result, this technology is evolving rapidly, and it will be no surprise that the future of digital business shall be in cloud computing platforms with a potential to restructure the entire ICT infrastructures for any business in coming years

Cloud-computing industry is rapidly growing and can be categorized as a new arena for the cybercrime. We are aware that Cyber criminals are always in search of new ground to play on, in 2013 Chinese group of hackers exploited Dropbox services, a cloud-based file sharing system with client applications installed at end users machine like mobile, tablets, and personal computers, to distribute malware to conduct Distributed Denial of Service (DDoS) [1]. As we are aware that with every technological invention, challenges of its security increases. With regards to cloud computing, it can be claimed that it is a huge opportunity for the people involved in cybercrime and a challenge for a security examiners/practitioners/auditor. In terms of forensics in cloud computing, even though it shares the common foundation with traditional forensic practices, it has its own unique barriers, challenges, and techniques [2]. From the very beginning due to the complex architecture of cloud computing, the storage ecosystem has been challenging for forensic examiners to acquire and analyze the evidence as compared to the traditional digital forensic process. This has been ambitious to investigate, as at some stage with cloud storage it is tough to get accurate details like data storage detail, data ownership, data integrity, etc. which can be questionable in courtroom, and it is equally essential to have a contemporary examination of the type of evidence that remains on end users devices and location of the data in the user machine while accessing cloud data [3].

The research presented here is focused on digital forensic of client nodes, which access the object-based cloud storage via the client application, or API provided by the cloud service provider to access the storage unit, which serves as the endpoint for data storage. To represent the scenario,

we have designed the simulation environment within Virtual box with guest Operating System Windows 7 OS which actively communicate with Object based cloud storage provider Digital Ocean Space [4], Scalable Cloud Object Storage by Rackspace [5] and IBM Cloud Object Storage [6] via client application Cyberduck [7] installed at the end user machine. Cyberduck was selected as a client application as all three-cloud storage service providers have recommended it and officially presented guidelines for setup as a client application for MAC and Windows system [8][9] [10]. During this research, we analyze the data remnants in the client's system that is of forensic interest, which is generated during the entire process between object-based cloud storage and the client machine.

1.1 Motivation

Cloud storage has made the computing cycle much easier and more interesting to individuals with implanting CDN network, pay as you go, on-demand service, etc. and finally an open ground with much more opportunity to conduct malicious activities by using infrastructure in clouds. This has resulted for individuals or group people with malicious intent can gain access to powerful computation capacity to play with. There are many more incidents in the past couple of year where attackers get into the cloud storage via end users' machine. Deloitte, one of the worlds big four accountancy firm, got hit by cyber-attack which remains unnoticed for a month, the hackers got access in the email system which is stored in Azure cloud service provided by Microsoft [11]. These days' hackers are using cloud services to distribute the malware easily among many end users devices like Dropbox has been used in targeted attacks for command and control purposes where attackers have signed into Dropbox with legit credentials [12]. Similarly, security researchers claim that hacker's activities on distributing their malicious product via cloud storage services are increasing these days as compared to the traditional way of distributing malware via their hosted website as these sites are easily detected and blacklisted [13]. We come across many such incidents in which, the prime victim of the attacker is always an end node, which acts as the bridge to attackers to conduct the malicious activities. It can claim that end node holds immense space in cloud computing and they are the primary target of attackers in the majority of the case.

With regards to the forensic in cloud, in the time of incident, forensic investigator must keep the end node in equal priority. Significant amount of forensic analysis needs to be conducted in the

client node as well during the time of acquisition of digital forensic evidence of interest. Client machines are the most essential device to trace the criminal activities as well as the most vulnerable part of cloud computing as compare to the sophisticated architecture of cloud computing. Forensic in end nodes can help the forensic investigator to collect much more trustworthy and reliable evidence of forensic interest during the time of the incident.

1.2 Scope

The research presented with this thesis is based on forensic investigation of client machine to identify/collect the range of artifacts arising from the user actions, which is of forensic interest during the process of accessing the cloud storage unit via client application. Such analyzed artifacts and devised process during this research will assist forensic examiner, academician, and practitioners in real-world investigation for the similar kind of cloud storage provider and client applications.

1.3 Problem Statement

The goal of this research is to develop the technical analysis guideline on specified end user node to identify/collect the range of artifacts/data remnants arising from the user actions like installation of client application, login session, logout, running process, share ID/Name, Integrity check,

account passwords, account IDs, shared URL, upload, download, delete etc. which is of forensics interest during the entire process of accessing the remote cloud storage unit via client application installed in end user machine.

The aim of this research is to:

- Identify/Collect all possible Forensic artifacts (evidence data) that reside on user machine storage on installation of client application.
- Identify/Collect all the possible Network Forensics artifacts that can be observed in Internet packets passing while communication between user end and cloud service provider.
- Identify/Collect all the possible Forensics Artifacts that relates to the volatile memory of user machine during the time execution of client application to access cloud storage unit.
- Identify/Collect all the possible Forensic Artifacts that relates to the change on data throughout the process of data transfer like uploading, downloading, and deletion of files.
- Identify/Collect all the Forensic Artifacts that related to any modification in timestamp/metadata during the process of data communication between client application on user machine and cloud storage.

1.4 Research Contribution

The outcome of our study after conducting the series of forensic analysis based on network forensic, volatile memory (Live acquisition), and static analysis on client machine to identify/collect the forensic artifacts due to the user actions can be helpful to the forensic investigator and researcher to conduct similar kind of study in coming days. The thesis presented here proceed with the analysis of client side of object-based cloud storage service providers i.e. Digital Ocean Space [4], Scalable Cloud Object Storage by Rackspace[5] and IBM Cloud Object Storage [6]. We have chosen to conduct a study on them, as we could not find any similar academic study conducted concerning on client side of these cloud storage service providers and we claim this as one of our major contributions.

We believe that the forensic procedure develop during this study will play significant role to understand forensic analysis from client's perspective and deliver more insight about the artifacts

thus generated in the client machine while working with object-based cloud storage and the forensic procedure devised in the thesis can be taken as reference to conduct similar type of study.

1.5 Limitations and Challenges

The research paper finds the range of forensic artifacts that is of interest during the forensic examination process, which is generated within clients end in our cases Windows 7 OS within VirtualBox while processing the data within the cloud-based object storage providers Digital Ocean Spaces, Scalable Cloud Object Storage by Rackspace and IBM Cloud Object Storage. The complete research is conducted within the client end in a virtually simulated environment. We are focused on client end with facts that at present millions of applications hosted in millions of servers around the globe are using cloud-based storage service as major data storage unit from multiple cloud vendors and serving such high increasing rate of internet users [14] every year via CDN network around the globe.

1.6 Thesis Structure

- Chapter 1 Motivation and Scope of our Research
- Chapter 2 Background Study
- Chapter 3 Framework, Tools that we used, and Experimental Setup
- Chapter 4 Research Methodology of Study
- Chapter 5 Result and Analysis
- Chapter 6 Conclusion

2.0 Background Information

This section consists of a brief discussion on digital forensic, cloud computing and cloud forensics. Digital forensic is a process of recovery and investigation of facts about digital evidence that is of forensic interest found on digital storage media or any device that possess the capability of computing. According to NIST [15], digital forensics comprises of following phases:

- **Collection:** Extraction of digital evidence from possible sources of relevant data with preserving the integrity of data.
- **Examination:** Processing of collected data or extraction and inspection of data with preserving the integrity.
- **Analysis:** Analyzing the results of the examination to derive the useful information that is of forensic interest.
- **Reporting:** Reporting the results of the analysis with detail information of the entire process conducted like tools used and procedure followed as well as recommendation for improvements.

Authors Keyun Ruan, et al. [16] define cloud forensics as "*Cloud forensic is a subset of network forensics deals with forensic investigations of networks and based on broad network access. Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing*". In short, we can define cloud forensic as a cloud computing and the network forensic as cloud computing is on-demand service via Internet.

NIST defines Cloud Computing as "*Cloud computing is a model which provides a convenient way of on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction*" [17]. In general cloud computing provides three significant services [17]:

- The Software as a Service (SaaS) model where the customer rents software for use on a subscription or pay-per-use model.
- The Platform as a Service (PaaS) model where the customer rents a development environment for application developers.
- The Infrastructure as a Service (IaaS) model where the customer rents the hardware infrastructure on a subscription or pay-per-use model and the service can be scaled depending upon demand.

Cloud storage services can be considered as type IaaS, provides end users with storage space that can be accessed through web browser, client application i.e. numbers of application for several types of end user devices like PC, smartphones, Tablets etc. Cloud storage mainly used as Cloud Sync, Cloud Backup, and Cloud Storage.

Cloud Sync is the services, which sync the local storage with the storage on other machine or cloud like Dropbox, iCloud, OneDrive, Google Drive etc. Cloud Backup these services work automatically as background daemon and backup all the changes made to the selected data for backup to cloud like Backblaze Cloud Backup, Mozy, Carbonite etc. Cloud storage is a service, which provides the endpoint for data storage via APIs, CLI, applications on demand on pay as you go mode like Amazon S3, Digital Ocean Spaces, Scalable Cloud Object Storage by Rackspace and IBM Cloud Object Storage [18].

The major focus of this research study is on working with object-based cloud storage. Object based cloud storage is an approach which managed data as objects where each object typically includes the data itself, a variable amount of metadata and a globally unique identifier [19]. In terms of cloud storage object storage is the storage and retrieval of unstructured blob of data using an HTTP API where entire object is deal over Internet instead of breaking the files down into blocks. These objects can be file, logs, picture, video etc. and are unstructured, as they do not follow any schema or format [20].

2.1. Cloud Computing Architecture

Cloud computing architecture consists of two major components Frontend and Backend that is connected via Internet. Frontend is are also known as cloud client which includes servers, thin and fat client, tablets, mobile devices, and personal computers in other words we can say all end users' devices. Frontend mainly communicates with backend to access multiple cloud services like SaaS, PaaS and IaaS via middleware or web-browser or virtual session through Internet.

Whereas, the major function of the back-end is to facilitate the services requested by front-end including data security, redundancy, scalability as well as provide the middle-ware that would connect devices and maintain communication between front-end and back-end.

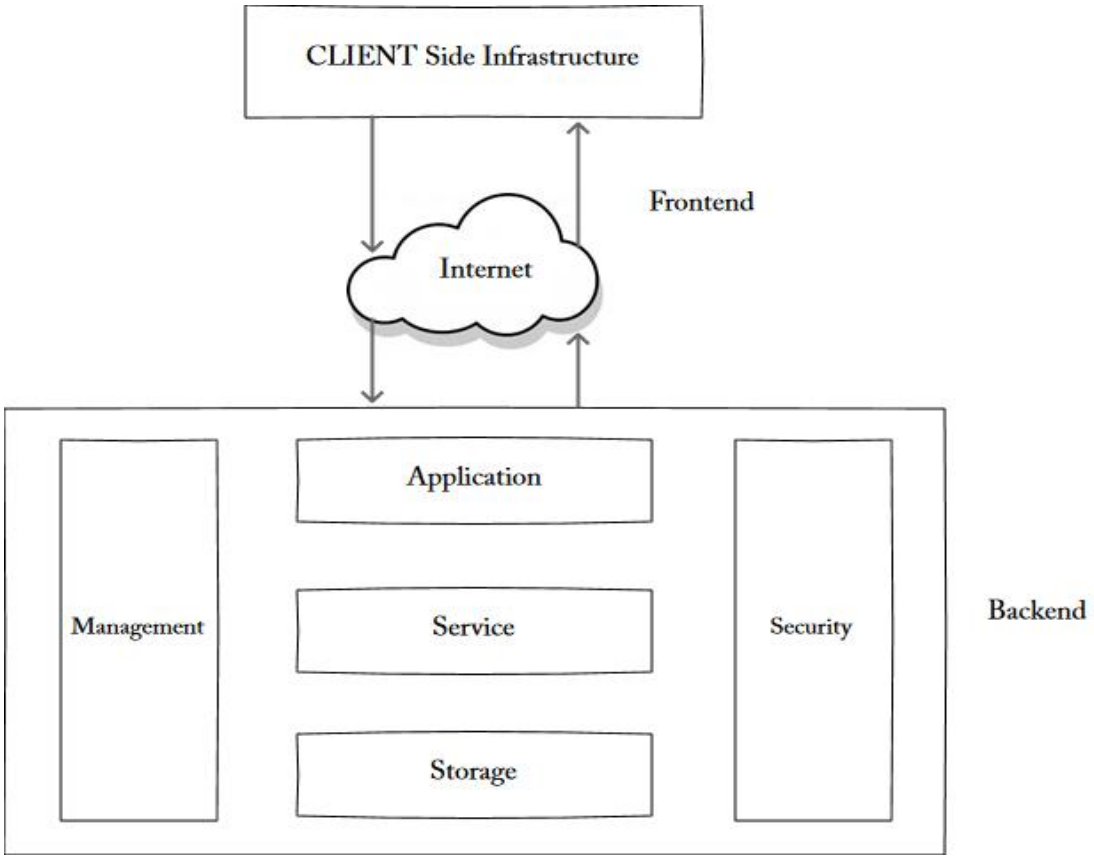


Figure 1. Cloud Computing Architecture [21]

2.1.1 Theoretical and Technical Background

The goal of Digital forensics is to conduct an organized and structured investigation to preserve, identify, extract, document and interpret digital information that is then utilized to prevent, detect and solve cyber incident. Typical digital forensic consists of four steps [22]:

- Preserving the data
- Acquiring the data
- Authenticating the data
- Analyzing the data

Here in this research moreover we are dealing with Network Forensics and Windows Forensics.

2.1.2 Network Forensics

Network Forensics is defined as the process of capturing, recording, and analysis of all network events that can be presented as evidence during a security incident. As Simson Garfinkel network forensics can be done in two ways "Catch-it-as-you-can" and "Stop, look and listen" [23]. In this research, we are following the Catch-it-as-you-can approach as it deals with the capturing all packets that are originated or passing through host or any device that is connected to the network and result can be stored for later analysis. Whereas, with Stop, look and listen approach analyzes each packet in memory, requires less storage and its faster processing compare to Catch-it-as-you-can.

We believe that the evidence we collect from the network forensic will have a significant value as we are going to upload and download between cloud storage and client machine. During this process, we can come across a number of valuable data exchange like username, password, data type, a protocol used for data communication, session id that can be accounted for as important evidence during a security incident.

2.1.3 Data acquisition

Data acquisition is the process of collecting digital evidence from computer media like hard drive, thumb drive, CDROM, removable hard drives, servers, and other media that stores electronic data. Two major types of data acquisitions [24]:

- Static acquisition
- Live acquisition

The static acquisition is the process of acquiring digital evidence after shutting down the system when a system is seized during a cyber incident. Normally done by making the duplicate copy of the disk by maintaining the integrity of disk. All examination is done on duplicate copy to collect the evidence from web browsing, file fragments, network connections, opened files, user login history etc. In short gives the statics about the activities performed on victim system before shutting it down [24].

The live acquisition is the process of capturing the digital evidence when a compromised system is functional or also known as capturing the volatile memory from the system. The evidence data can be running process, logs, registered services, unencrypted version of encrypted files, network connection status, username/password, an executable file that is running, logged in user including remote users, open files or memory dumps [24].

2.1.4 Windows Forensic

The major part of this thesis is windows forensic, as we are concerned with the windows PC's at end users who actively communicating with cloud storage. Windows forensic focuses on building in-depth digital-forensics knowledge of Microsoft Windows OS [25]. Some of the key artifacts which is forensically important in windows system as follows:

- **Windows registry key**: Microsoft defines "*A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files containing backups of its data.* "Also, most of the supporting files for the hives are in "*%SystemRoot%\System32\Config*" directory [26]. Below listed are the standard hives [27]:

(a) NTUSER.DAT: Related to users' activities.

(b) SAM: Information about users and groups (Security Account Manager)

(c) SOFTWARE: Information about all software items in the system.

(d) SYSTEM: Information about all hardware item in the system.

(e) Security: Information about security.

- **Shortcut:** Symbolic link to the program, which ease the users to locate the programs in any folder start bar, Taskbar, Desktop or other location in system [28]. Forensically it provides significant information about the location of the program even it is removed from the system.
- **Jump Lists:** Allows to view recent documents in a program pinned to the taskbar, as well as recently visited files with respect to program [29].
- **Log File:** Provides the detail list of application information, system performance, or user activities [30].
- **MFT:** MFT is the location NTFS keeps tracks of the contents of a volume. It is an index of all the files containing a file name, file metadata, file pointers and attributes. In forensics, it plays a vital role to collect the evidence related to the files [31].
- **Recent Files:** Contains the links to the recently accessed files or folder in a system.

2.2 Literature Review

Cloud forensic, investigation needs to be conducted on both ends client end as well as server end. We have already discussed it in above section and our focused in on client machine forensic study with a confident that traces of used services will remain in the client machine due to user activities, which holds equal worth in terms of evidence collection during a cyber incident. In a number of studies made by many academicians within client-side they have succeed to achieve the success as compared to the distributed nature of cloud computing where conducting a cloud forensic is a quite tedious job. Plenty research had been done in similar type subjects by the numbers of authors

like Dropbox, MEGA, OneDrive, Amazon S3, and Google Drive whereas as we already mentioned in our introduction section such type of forensic study is not conducted for Digital Ocean Space, Scalable Cloud Object Storage by Rackspace and IBM Cloud Object Storage.

2.2.1 Dropbox

Dropbox is a file hosting service where you can store and share files, collaborate on projects, store and access files from anywhere like from computer, mobile phone, tablet. Files modification can be done from any device via client application with ability to sync across all devices [32]. Dropbox is popular cloud storage technology as it gives end user free service with 2GB of data storage and numbers of researchers have conducted forensic study to collect the digital evidence from end user machine. Like, Frank McClain pointed in the analysis of Dropbox Forensics various traces in client machine can be found like installation directory, changes in registry during installation, network activity, databases, logs, and uninstallation details [33].

Similarly, on other research about "*Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices*" authors Farid Daryabara, et al. able to find artifacts of forensic interest, such as information generated during login, uploading, downloading, deletion, and the sharing of files on IOS and Android platforms [34].

2.2.2 MEGA

MEGA is cloud storage and file hosting service offered by Mega Limited it offers 50GB of free online data storage and support for sharing and mobile uploads [35]. According to Farid Daryabar, et al. in "*Cloud storage forensics: MEGA as a case study*", MEGA alternative to Google Drive, Dropbox, and OneDrive. Authors managed to identify the range of artifacts arising from user activities, such as login, uploading, downloading, deletion, and sharing the files, which could be forensically recovered on android and IOS platforms [36].

2.2.3 OneDrive

OneDrive is Microsoft service for hosting files in the cloud, it offers services like store, sync, and share files over Internet [37]. Authors Farid Daryabara, et al. in "*Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices*" have made

research about the identification of artifacts that is of forensic interest such as information generated during login, uploading, downloading, and the sharing of files via cloud client applications on Android and IOS Platforms [38].

2.2.4 Amazon S3

Amazon S3 provides the end user simple web interface that can be used to store and retrieve any amount of data, at anytime from anywhere on the web. It provides highly scalable, reliable, fast. Inexpensive data storage services [39]. Authors Hyunji Chung , et al. analyzed four cloud services Amazon S3, Google Docs, Dropbox, and Evernote in their study "*Digital forensic investigation of cloud storage services*" [40] in search of data remnants left by client application and come up with a process model for forensic investigation of cloud storage services and reported analyzed services may create different artifacts depending on the specific features of the services .

2.2.5 Google Drive

Google Drive is one of the widely used cloud storage service at present time to shares files and folders, stores any file like photos, designs, videos and more with ease to reach stored files from any smartphone, tablet, or computer with the help of client application. It gives user 15GB of free storage with a Google account [41]. Many researchers regarding the analysis of data remnants related to Google Drive have conducted Numbers of research. Authors DarrenQuick, et al. in the study "*Google Drive: Forensic analysis of data remnants*" they manage to identify the artifacts on client machines like computer hard drive and Apple iPhone3G after the use of cloud storage[42] . Similarly, author Ming Sang Chang in study "Forensic analysis of Google Drive on Windows" is able to trace the data remnants left on client devices while using Google Drive via multiple Internet browser on platform Windows XP, Windows 7, and windows 8 [43]. Author Tariq Khairallah in study "*Cloud Drives Forensic Artifacts A Google Drive Case*" able to discover and collect the artifacts left by cloud storage applications even after the deletion of Google drive client application on Windows 10 operating system [44].

Above mentioned are well known cloud storage services provider where we found numbers of researcher have worked to gather traces of data remnants that is generated on client machine that can be presented as the digital evidence during cyber incident. Similarly, we can find couple more

literature for multiples types of cloud storage on multiple platforms on client end. Like, authors, Fabio Martaurana made the digital forensic analysis in windows 7 systems with the help of set of traditional forensic tools set to identify the potential forensic artifacts from the use of Google Docs, Dropbox, Picasa Web, and Flikr that is locally synced in the client machine and able to demonstrate that potential evidence can be found in logs, temporary files, internet cache, navigation history, downloads and cookies of web browsers [45].

SeyedHossein Mohtasebi, et al. in "*Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud,and pCloud*" have made research about the possible changes on uploaded and downloaded files metadata on windows 8.1 and iOS 8.1.1 devices [46].

All above mentioned research work is concluded with successful results with number of scopes for future enhancement. The literature presented here will be very helpful to conduct the research as we already mentioned in above section the research presented is focused on client side of cloud-based object storage of Digital Ocean Spaces recently introduced by Digital Ocean as object-based cloud storage service, Scalable Cloud Object Storage by Rackspace and IBM Cloud Object Storage.

3. Methods and Experiment Setup

In this section we have brief discussion about the forensic framework and lit of tools that is used to conduct this study.

3.1 Digital Forensic Framework

To conduct our experiment we are using the cloud forensic framework introduced by Martini and Choo [47] can be claimed as the first digital forensic framework designed to conduct both client and server investigation and is been validated by the authors using ownCloud (Martini & Choo, 2013), (Martini & Choo, 2014b), (Martini & Choo, 2014c), and by Thethi and Keane (2014) on EC2 cloud [46]. This forensic framework moves on to four phases.

- **Evidence Source Identification and Preservation:** This phase is associated with the identification of the potential sources of relevant evidence that can be desktop computer, laptops, or mobile devices. After identifying the sources, it then deals with identification of cloud service provider and processes the preservation of potential evidence. Regardless of the identified sources of evidence, forensic investigators need to ensure the proper preservation of the evidence.

- **Collection:** This phase deals with the actual data capturing. The collection part first deals with the seizure of client devices and then in second phase it deals with the collection of server data. In our thesis we are only focused on collecting the data from client devices like events logs, communication logs, data from hard disk and memory dump preserving the integrity of data throughout the entire process [48].

- **Examination and Analysis:** This phase is concerned with the examination and analysis of forensic data. Based on the examination and analysis of physical devices this can goes up to multiple iterations [48].

- **Reporting and Presentation:** This phase is associated with the legal presentation of the evidence collected including all the processes, tools and applications used and any limitation to prevent false conclusions [48].

3.2 Forensic Process in Experiment

As mentioned above our thesis is following the cloud forensic framework introduced by Martini and Choo [47]. We have managed to conduct forensic analysis as Network Forensics, Live acquisition, static acquisition, and Windows Forensics.

- **Network Forensics:** We manage to capture and analyze network traffic for potential forensic evidence during the process of communication between client machine and cloud storage service provider by isolating the client machine from other external connectivity to avoid any kind of unwanted data that could modify the evidence.
- **Live Acquisition:** We managed to dump volatile memory data (RAM) and analyze it to achieve the potential evidence that is admissible to court. This is step performed by making a very minimum amount of changes in the system by accounting all the changes made to the system.
- **Static Acquisition:** During this step we managed to acquire the entire hard disk (unallocated spaces) of the system in multiple steps of experiment like uploading, downloading, deleting and installation of client applications.
- **Windows Forensics:** This step relates to the depth forensics analysis of Windows 7 Operating System to gather all the potential forensic evidence that is generated due to user activities based on Windows forensics manners.

3.3 Forensic Tools

To conduct this research work we have used multiple forensic tools, which has been frequently, used by forensic expert similar type of study. We will discuss about each of them in this section under each forensic process that we are going to present in this thesis.

- **Network Forensic**

  During this phase of our forensic analysis we used well-known tools Wireshark and Network Miner to capture packets during communication between cloud storage client application and cloud storage service providers.

  a) **Wireshark:** Wireshark is widely-used network protocol analyzer as it does the deep inspection of protocols, live capture and offline analysis, multi-platform (Linux, macOS, Solaris, FreeBSD and many others), GUI to visualize the capture data, captured files with gzip can be decompressed on the fly and many more [49].

- **Live acquisition**

  During this step of our experiment we manage to dump the contain of RAM by using following tools:

  a) **FTK Imager (v3.4.2):** One of the popular tools used by forensic investigator to preview data and imaging tool used to acquire data (evidence) in a forensically sound manner by creating the copies of data maintaining its integrity. FTK Imager can create forensic image, preview files and folder, preview contents, mount an image for read only view, export files and folder, recovery of deleted files and folder, create hashes of files, and generate hash reports [50].

  b) **Volatility (v2.6 windows standalone):** It is the open source software program for analyzing RAM in 32bit/64bit system available for Linux, Windows, Mac and Android systems. It can analyze raw dumps, crash dumps, VMware dumps (.vmem), virtual box dumps and many others [51][52].

- **Static/Post-mortem acquisition:** As already discussed in above section we acquired entire hard disk of the system during different phases of analysis and tool used for disk acquisition is FTK imager.

- **Windows Forensics:** To analyze the files and folder under Windows 7 OS we used multiple industry standard tools that has been used by forensic investigator for successful output. Below mentioned are the tools with brief description of each.

    a) **FTK Imager:** One of the popular tools used by forensic investigator to preview data and imaging tool used to acquire data (evidence) in a forensically sound manner by creating the copies of data maintaining its integrity. FTK Imager can create forensic image, preview files and folder, preview contents, mount an image for read only view, export files and folder, recovery of deleted files and folder, create hashes of files, and generate hash reports [50].

    b) **Autopsy (v4.11.0):** Digital forensic platform and graphical interface to the *Sleuth Kit*. It been widely used by law enforcement, military, and corporate investigator and used a recovery tool to recover the files and folder from hard disk, memory card, external drive etc. Some of the modules of Autopsy are Timeline Analysis, Keyword Search, Web Artifacts, Data Craving, Multimedia, Hash Filtering and Indicators of Compromise [53].

    c) **Mft2csv:** Tool for parsing, decoding, and logging information from the $MFT to a csv as having data in csv is very convenient for further analysis [54].

    d) **Microsoft Excel**: Developed by Microsoft we used it to read the csv file generated by Mft2csv.

    e) **JumpListView:** Tool that displays information stored in the Jump Lists of Windows 7/Windows 8 OS. Information like filename that user open with date/time with associated program ID that opened the file [55].

    f) **RecentFilesView:** Tool that display the list of all recently opened files and allows you to delete the unwanted filename entries [60].

g) **AccessData Registry Viewer:** Tool to view the contents of Windows registry can visualize registry files from any system, provides access to registry-protected information like username and password. And finally, this tool is not free we need a license to use it [56].

h) **Windows System State Analyzer:** This tool allows to compare the two snapshots taken at different time, like compare the snapshot before and after the installation of any software in a windows system [57].

i) **Windows System State Monitor:** This tool allows you to monitor the areas of system like registry, services, and drivers and once the monitoring is enabled in the system it will logs all the changes made to the system [57].

3.4 Workflow

We begin our analysis by spinning a VM on Virtual Box with Windows 7 OS. After installation of necessary tools, we begin our analysis with capturing the traffic on LAN interface of VM. Next step performed is started the Cyberduck client application on VM and required login detail is supplied to connect to the remote object-based cloud storage we have presented the login procedure in Appendix A. Once we confirmed successful login we begin to synchronize local directory with remote cloud storage unit. During synchronization process we manage to transfer multiple files from local machine to remote cloud storage the list of all files name md5sum are presented in Table 1, Table 2, and Table 3. Once the file transmission is confirmed through client application then memory dump was initiated with FTK Imager for the analysis of volatile memory md5sum of each memory dump for individual machine associated with different storage service provider in our simulation environment can be found in Table 6. After this step we stopped the network capture for first phase and the file was saved with .pcap format for further analysis we have presented all .pcap file name with md5sum in Table 5 and proceed with disk acquisition 2. The second part of our analysis is capturing the evidence related to deletion of files and logout of procedure. As presented in our workflow diagram we begin with network capture 2 and from Cyberdeck client application console we deleted file and proceed with sync

with local folder. After this we proceed with the logout from remote cloud storage unit via Cyberduck client application and we initiated the volatile memory dump 2 to capture the evidence related to deletion of file and logout activities. We stopped the network capture 2 and saved the file into .pcap file format. Finally, with the help of FTK Imager we proceed with disk acquisition 2 to collect the artifacts related to the deletion on object in terms of local storage.

We repeated same process for all three cloud storage services that we have analyzed during this thesis. In brief we have presented this work flow in below Figure 2.

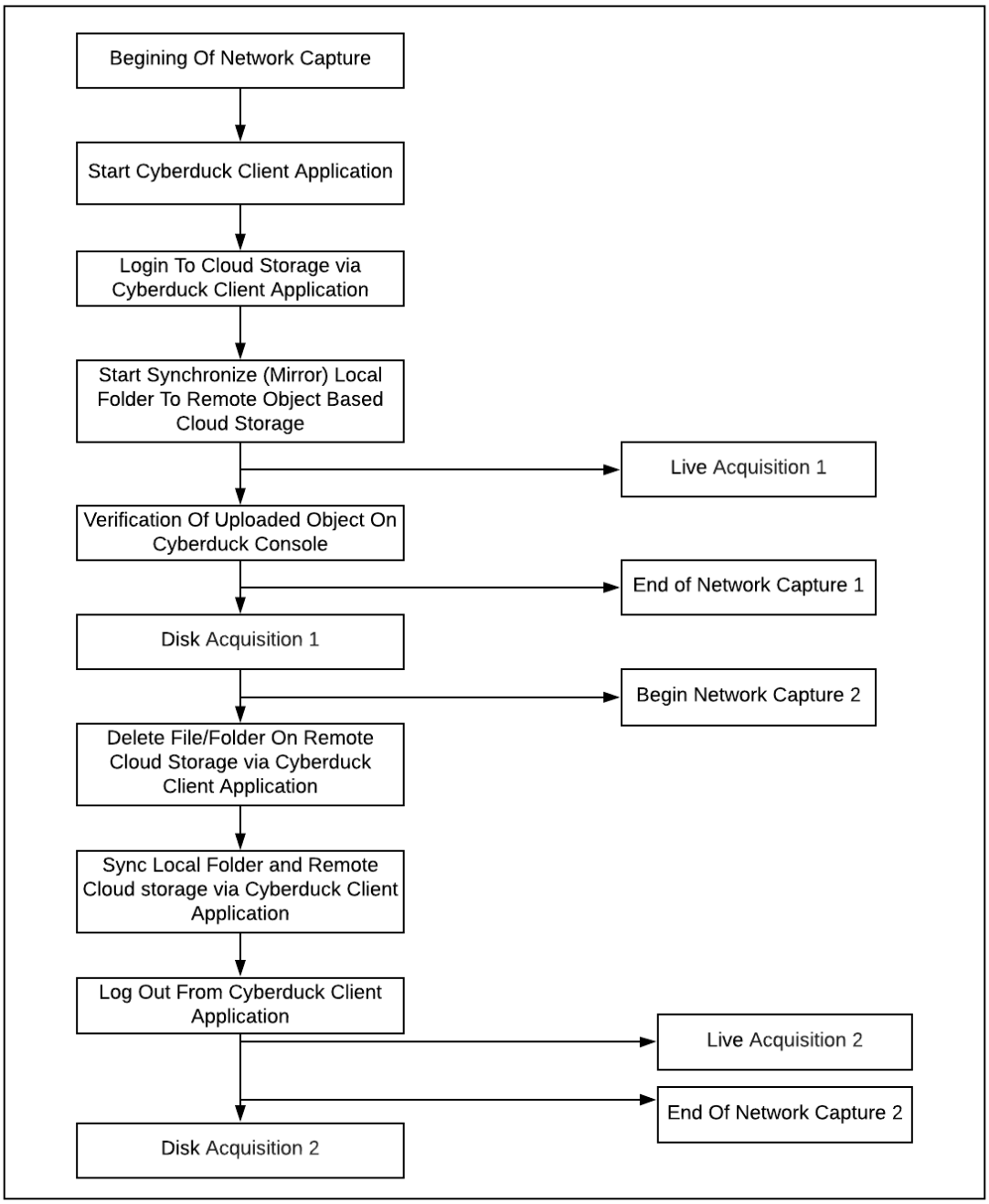


Figure 2. General work flow diagram

3.5 Study Cases

We have three cases of study for all three Cloud Storage service providers. We have prepared three different systems for individual cloud service provider. Then on each system we performed Network Capture via Wireshark and saved the .pcap file for further analysis, Memory Dump (Live forensic) via FTK imager running on external drive and finally we acquired hard disk for static analysis from individual system that corresponds to individual cloud service. Network capture and Memory dump was done side by side at the same time while Cyberduck Client application is in action like login in to remote cloud storage service provider, file transfer (upload and download) between client machine and cloud storage. To maintain the Integrity, we have managed to take the MD5sum of both memory dump and captured .pcap file.

We begin our study by analyzing the .pcap file for individual cloud service followed by the analysis of memory dump with volatility and FTK Imager and finally disk analysis for windows forensic to collect all related forensic artifacts. Below given tables contains the file name and md5sum hash of each file that we transferred each remote object-based cloud storage during the analysis of each case.

S. N	File Name	MD5Sum
1	sample1_zip.zip	da87f50c9267efec0d30620b517f194a
2	sample2_docx.docx	30ac5dcee7208b6fa6febf10708a4df9
3	sample3_picture.jpeg	490fbaff4ba2301d35c96b1eb2167efa
4	sample4.txt	B71bfde4dbeb91919b91bb89e27409d4

Table 1. DO Spaces file names with md5sum

S. N	File Name	MD5Sum
1	sample1-Rackspace-txt.TXT	12008597e3a51acdde7114249f9d1c28
2	sample2-Rackspace-pdf.pdf	3159999a42fbb864e72025b180b3723d
3	sample3-Rackspace-jpg.jpg	f8001686e624353f792a394e07263644
4	sample4-Rackspace.tar.gz	B55e09c19c8f10125e8137f08d560145

Table 2. Rackspace Cloud file names with md5sum

S. N	File Name	Md5sum
1	sample1-IBM-COS-TXT	a9ae8a1317db155001a234335af7b8ca
2	Sample2-IBM-COS.jpeg	D0c93df1d49ce699d3542059f9801cf6
3	Sample3-IBM-COS.docx	188204e37bd808f0a01f5984abc36515
4	sample4-IBM-COS-pdf.pdf	f195d7d2ab7f403a1a87164124b170fe

Table 3. IBM COS file names with md5sum

4. Research Methodology of Study

We managed to create the guidelines for forensic researcher, academician, and investigator based on following categories.

- Installation Artifacts
- Network Forensics
- Live forensic
- Static acquisition

4.1. Installation Artifacts

We manage collect the list of artifacts that is related to the installation of client application on Windows 7 OS with the help system state monitor and windows system state analyzer to collect the Cyberdeck client installation artifacts on Windows & OS. With the help of these tools the artifacts are collected based on changes made on the system during the installation process as follows:

- File System
- Registry
- Services
- Drivers

To collect the artifacts related to the Cyberduck client installation, snapshot was taken with the help of windows system state analyzer before and after the installation of Cyberduck client application and the snapshot was compared as shown in below Figure 3. At the same time,

windows system state monitor was started to monitor the changes made on File system, Registry, Services and Drivers during the installation process of Cyberduck client application.

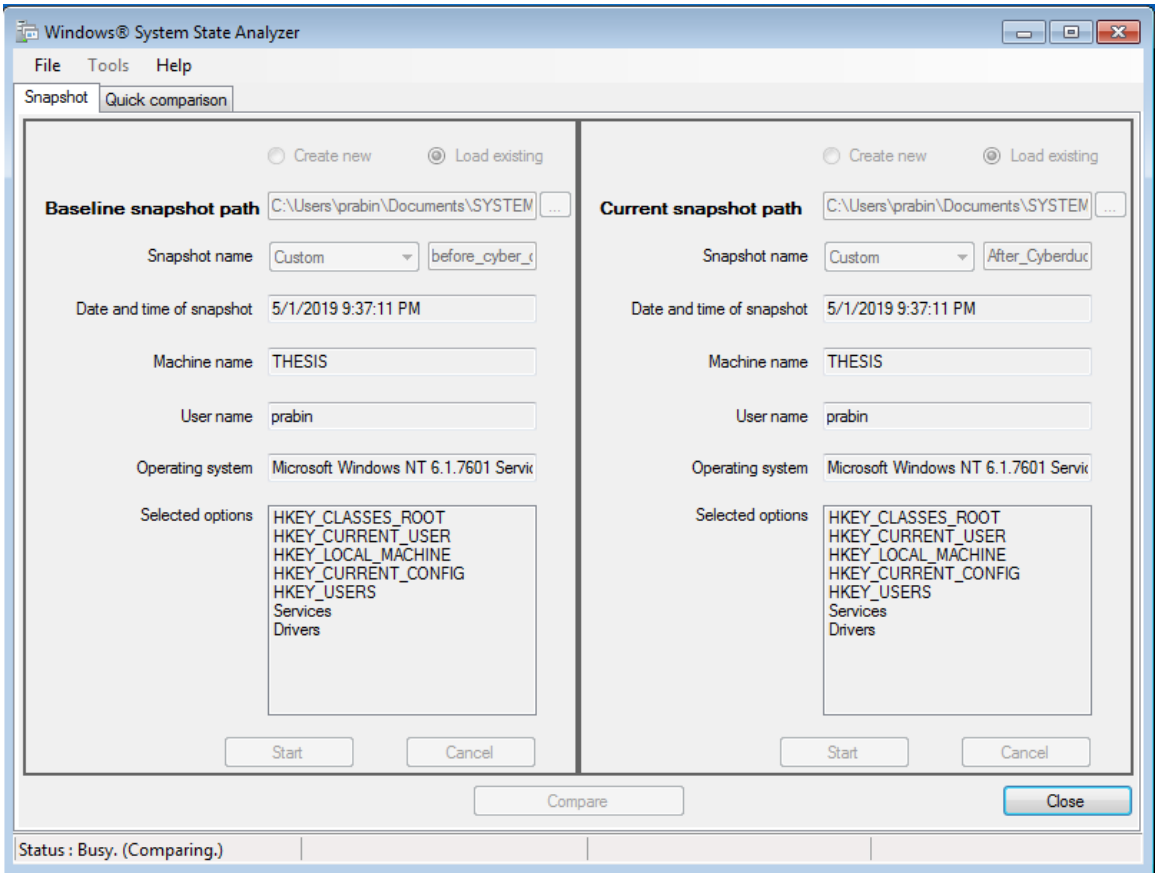


Figure 3. Windows System State Analyzer Comparison

After the installation process completed report was generated from Windows System State Monitoring and summary of report is presents in Table 4 below.

	Added	**Modified**	**Deleted**
Folder/Files	3862	1368	881
Services	7	9	0
Drivers	1	1	0
Registry Keys/Values	HKCR (2465) HKCC (0) HKCU (1030) HKLM (27241) HKU (1986)	HKCR (9) HKCC (4) HKCU (28) HKLM (466) HKU (36)	HKCR (43) HKCC (0) HKCU (46) HKLM (503) HKU (123)

Table 4. Summary Installation Artifacts

Here from Table 4, 7 different services added but our concern is with Bonjour Service. As per the Cyberduck it's for auto discovery of FTP and WebDAV services [7]. These services can give us the important insight during the forensic analysis. On browsing the path "C:\Program Files\Bonjour\" we manage to locate following files.

- About Bonjour.lnk
- dns_sd.jar
- mdnsNSP.dll
- mDNSResponder.exe

On digging manually for folders and files that is created during installation process under C:\Program Files (x86) \Cyberduck, we found 50 files and 3 directory that relates to the installation of Cyberduck.

4.2. Network Forensics Artifacts

We manage to capture the traffic and save .pcap files for further analysis during different states of analysis. We have divided network activities into multiple steps like file transfer and login as

the first part of our network dump. During second part we consider the network dump during the user action like file delete and logout from remote cloud storage. Cyberduck client application installation and file transfer process is presented in Appendix A. The Table 5 below consist of md5sum of network dump .pcap files for both network capture 1 and network capture 2.

Filename	**Md5sum**	**Associated Cloud Storage Unit**	**Network Dump Phase**
do_login_file_transfer.pcap	ad0191816aab7758264d8678e8a407f2	DO Spaces	1
do_file_delete_logout.pcap	68641c37a596f8a83e3f521772791d7a	DO Spaces	2
ibm_cos_login_file_transfer.pcap	827b3cb53d91fa7a8b27239fe2e7caa2	IBM COS	1
ibm_cos_file_delete_logout.pcap	3195c08ea3fae72303681201f504666e	IBM COS	2
rackspace_login_file_transfer.pcap	f8d91e3df62b1023a557252fdaa0ca39	Rackspace	1
rackspace_file_delete_logout.pcap	4e90ff43cb25f4c140a52b85b4232ff7	Rackspace	2

Table 5. md5sum for network captured .pcap files

4.2.1. Digital Ocean Spaces

The packet captured during the process of communication between Cyberduck client and DO spaces was saved on .pcap file format for further analysis. The saved. pcap file is loaded in to the Wireshark for analysis. Ongoing through the Wireshark console for TCP three-way handshake the first three (TCP SYN, TCP SYN/ACK, TCP ACK) between Cyberduck Client and DO spaces we found Client Hello (First TLS packet) with TLSv1.2. we continue our search with filter TLS On

Wireshark we found TCP three-way handshake sequence on Wireshark console as shown in below figure 6. On destination column we can see the remote server IP address (5.101.110.225).

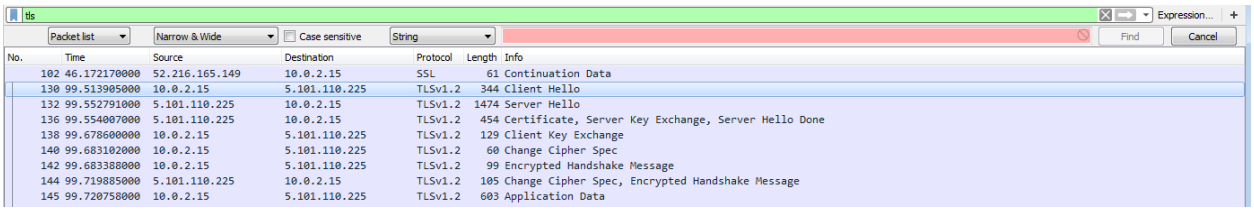


Figure 4. DO TCP three-way handshake during login

Further we proceed with looking into Application Data to figure out the data transmission during the login process it is encrypted (http-over-tls). The login detail passed to the Cyberduck client is as follows:

- Server: ams3.digitaloceanspaces.com
- Access Key ID: N4I5QCSJ5EF3ZZLTS5L5
- Secret key: a1cfc6a7008180d78f12d1b1cec9618da67c52f1210c9a66

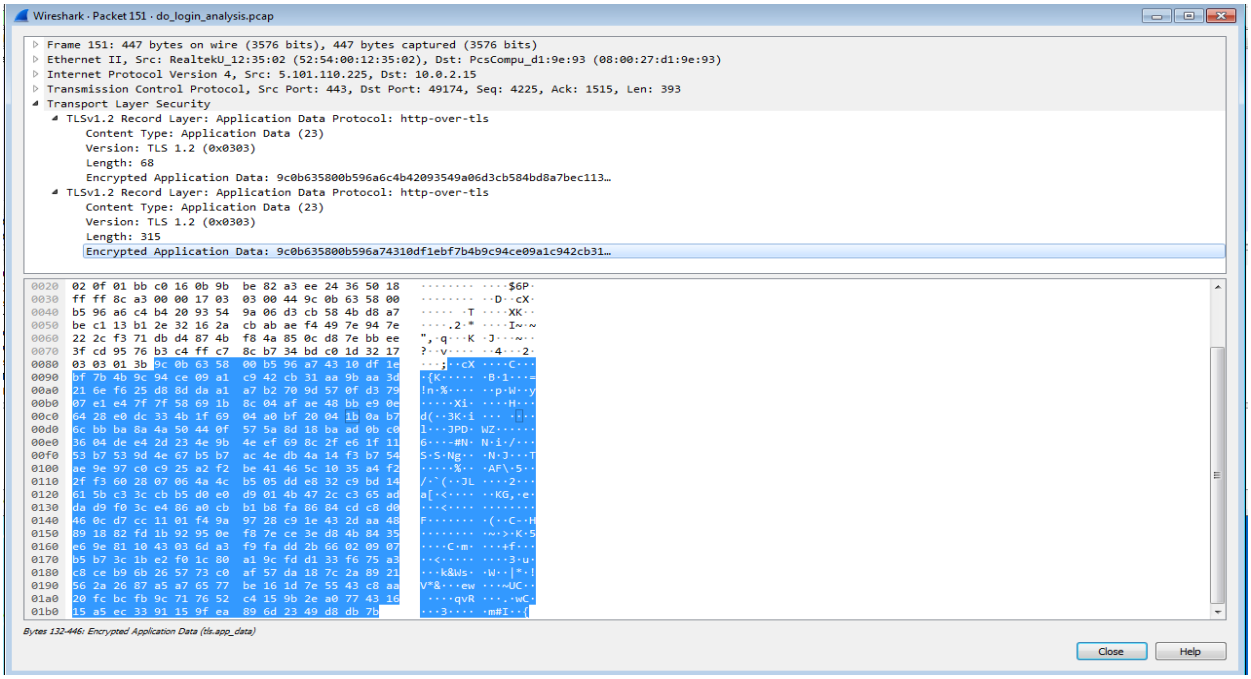


Figure 5. Application Data Analysis for Login

On following the TCP Stream, we succeed to find the endpoint for cloud storage server side *.ams3.digitaloceanspaces.com. We loaded the Wireshark with .pcap file captured during the file

transfer we figure out that it follows the same process for Three-way handshake as discuss in above section. We found the Application Data is encrypted with TLSv1.2.

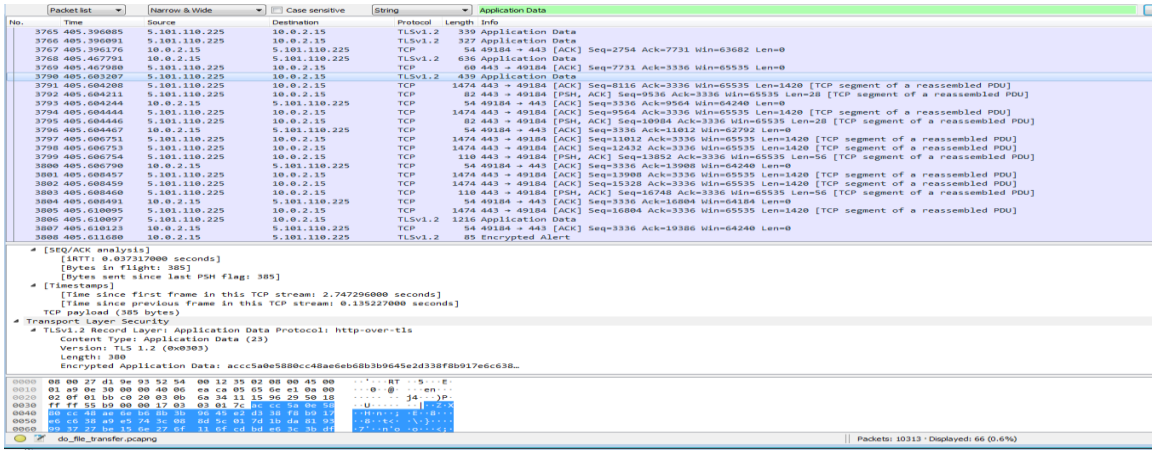


Figure 6. Application Data Analysis For data transfer

As everything is encrypted we could not see much things in object deletion process likewise while logging out from cloud we could see the TCP FIN initiated for the termination of TCP connection between client machine and remote cloud storage endpoint.

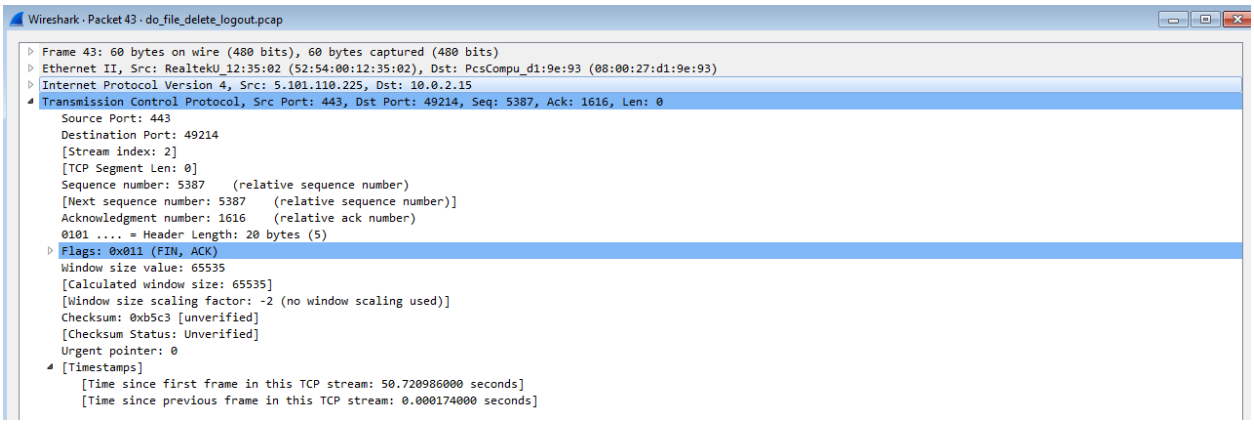


Figure 7. TCP Connection Closed Initiation between DO spaces and Local Machine

4.2.2 IBM Cloud Object Storage

With help of Wireshark packets were captured during login phase and data transfer each file was saved in .pcap format for further analysis with md5sum hash to maintain the integrity.

The login details for IBM COS provided for the Cyberduck Client is as follows:

- Endpoints: s3.ams03.cloud-object-storage.appdomain.cloud
- Access Key id: 6409e863e6ed4227937fe0f5915a5983
- Secret Access Key: a1cfc6a7008180d78f12d1b1cec9618da67c52f1210c9a66

Same procedure was followed as in above section started our search with filter by searching for first TCP packet by adding the filter value *tcp.stream eq 0* on filter field in Wireshark GUI. On looking in to the DNS resolution with help Wireshark filter keyword dns managed to find the dns resolution for endpoint domain name and IP address. Ongoing through the application data field found all transferred packets are encrypted (http-over-tls) Finding is listed below.

- Encryption: TLSv1.2
- Contacted IP Address: 159.8.199.241
- Domain**:** s3.ams03.cloud-object-storage.appdomain.cloud

4.2.3 Rackspace Cloud Files

During the analysis of .pcap file for login and data transfer we could not find any different result as compare to the results mentioned in above sections for IBM and DO cloud storage. The findings for Rackspace cloud file are as below:

- Encryption: TLSv1.2
- Contacted IP Address: 166.78.226.217
- Domain**:** identity.api.rackspacecloud.com

4.3. Live Forensic

The image of physical memory was acquired with the help live FTK Imager installed in external drive. To meet the forensic standard knowing the fact acquisition in an untrusted environment and analysis on trusted environment. We moved the acquired Image of memory on trusted environment for further analysis by maintaining the integrity

Image Name	**Md5sum**	**Memory Dump Phase**
DO_memdump.mem	4b47f9aaf260dc4916a7a9f2f7cab991	1
IBM_COS_memdump.mem	A47598ab69649947958aac35f2b13139	1
rackspace-memdump.mem	8fe79c55267ac9a19f2e697946694ab1	1
ibm_logout_filedelete_memdump.mem	92f996a65511de8641acf3084fa95268	2
do_logout_filedelete_memdump.mem	aa85eb5ec233824ad46e29a26f527e21	2
rackspace_logout_filedelete_memdump.mem	9e332b93e9367f80f51cf7caf1d8f3e8	2

Table 6. List of Memory Images with md5sum

Memory dump was done while Cyberduck client application was running in the system with aim to capture the artifacts that can be found in volatile memory at the time of communication between client application and cloud storage while user activities like login to remote cloud storage unit, files transfer between local to remote vice versa as a first phase of dump whereas file delete and

logout during the second phase of dump. All acquired physical memory images from three individual system was captured as per our setup for Digital Ocean Spaces, IBM COS and Rackspace Scalable Cloud Object Storage (Cloud Files) during two stages of our analysis i.e for login and logout. To maintain the integrity, we took the md5sum of all physical memory images which is presented above in Table 6.

With the help of volatility forensic framework, managed to trace the process list, network connection, hostname, registry hive and some part of MFT record that is of forensic interest. During our analysis for coming sections Image info, process list, process privileges, hive list, and MFT on individual client machine where Cyberduck Client application is configured to access individual cloud storage of our interest. This analysis is all about collecting the artifacts related Cyberduck Client application on Windows 7 OS which holds same process for all three-client machine due to this we have presented the analysis process for single client machine. Whereas, for command netscan to view all network connectivity status a detail analysis is presented in network connection section for all three-local machine.

4.3.1 Image Info

With help of volatility command imageinfo brief information about the memory dump image was achieved. We followed [58] to find all necessary commands that we required during our analysis.

Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f DO_memdump.mem imageinfo

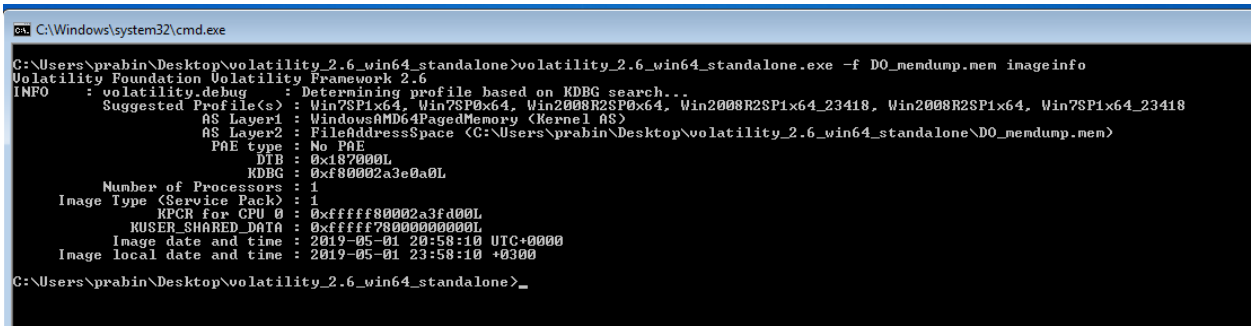


Figure 8. DO Memory Dump Image Information

In similar way with the help of command imageinfo image info for IBM COS and Rackspsce cloud files can be obtained.

4.3.2 Process List

Process list can be found with command pslist by running the command presented below the process ID for Cyberduck.exe was captured i.e 2032.

Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f Digital_ocean.mem pslist

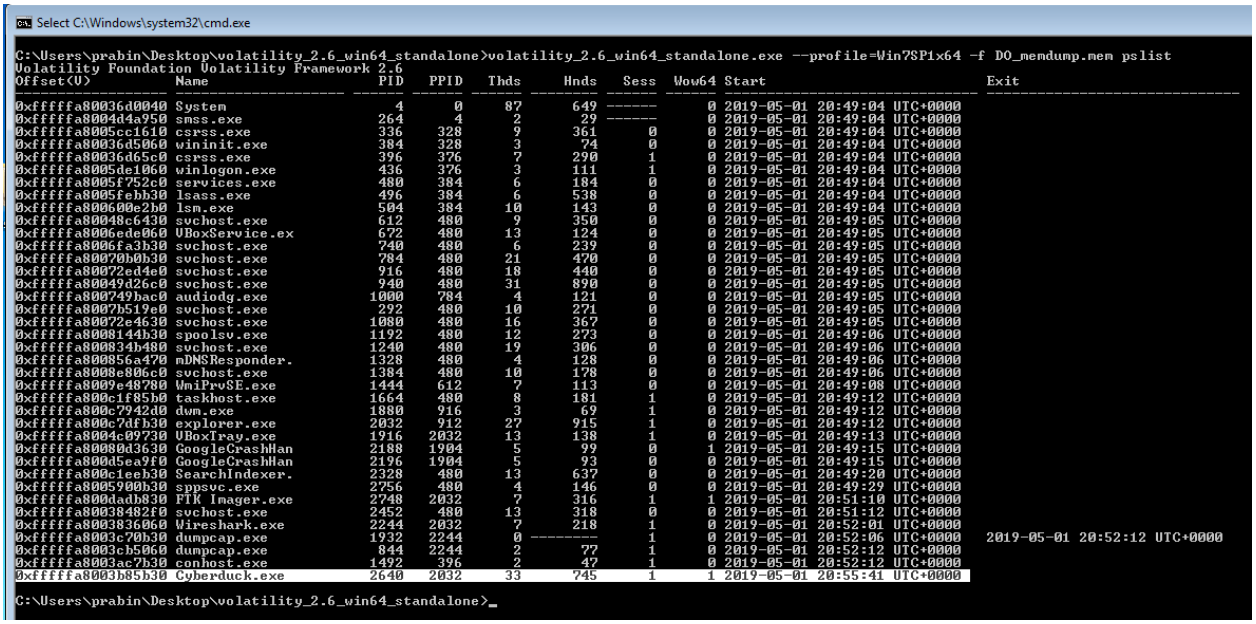


Figure 9. DO Memory Dump Process list with Cyberduck.exe process

4.3.3 Process Privileges

With command privs within volatility the list of privileges of the process that are associated with the process of Cyberduck.exe i.e 2032 can be determined.

Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f DO_memdump.mem privs -p 2032

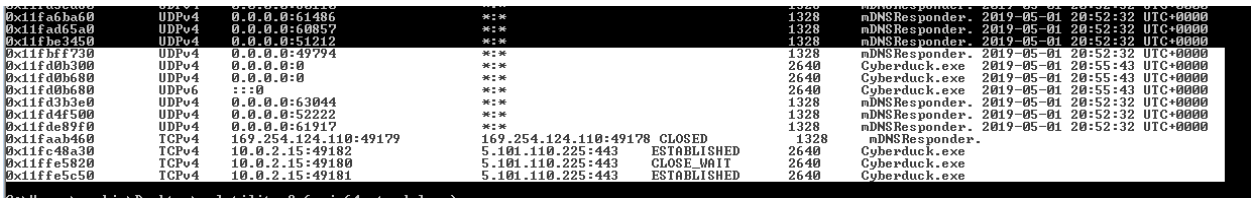
4.3.4 Network Connection

In this section we make analysis of network connectivity for each client machine which is associated with Cyberduck client application setup to reach the individual remote cloud storage unit.

4.3.4.1 Digital Ocean Spaces

Command

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f DO_memdump.mem netscan



0x11fa6ba60	UDPv4	0.0.0.0:61486	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fad65a0	UDPv4	0.0.0.0:60857	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fbe3450	UDPv4	0.0.0.0:51212	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fbff730	UDPv4	0.0.0.0:49794	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fd0b300	UDPv4	0.0.0.0:0	*:*	2640	Cyberduck.exe	2019-05-01 20:55:43 UTC+0000
0x11fd0b680	UDPv4	0.0.0.0:0	*:*	2640	Cyberduck.exe	2019-05-01 20:55:43 UTC+0000
0x11fd0b680	UDPv6	:::0	*:*	2640	Cyberduck.exe	2019-05-01 20:55:43 UTC+0000
0x11fd3b3e0	UDPv4	0.0.0.0:63044	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fd4f500	UDPv4	0.0.0.0:52222	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11fde89f0	UDPv4	0.0.0.0:61917	*:*	1328	mDNSResponder.	2019-05-01 20:52:32 UTC+0000
0x11faab460	TCPv4	169.254.124.110:49179	169.254.124.110:49178 CLOSED	1328	mDNSResponder.	
0x11fc48a30	TCPv4	10.0.2.15:49182	5.101.110.225:443 ESTABLISHED	2640	Cyberduck.exe	
0x11ffe5820	TCPv4	10.0.2.15:49180	5.101.110.225:443 CLOSE_WAIT	2640	Cyberduck.exe	
0x11ffe5c50	TCPv4	10.0.2.15:49181	5.101.110.225:443 ESTABLISHED	2640	Cyberduck.exe	

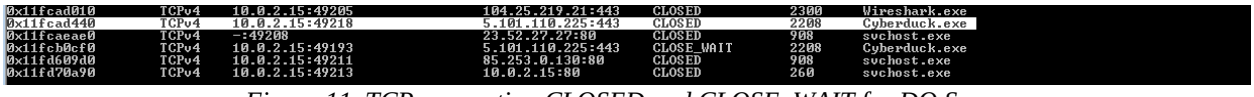
Figure 10. List of network connection associated with DO Spaces

Cyberduck Client Application have multiple TCP connectivity status like Established and Close Wait on different session with remote endpoint IP address 5.101.110.225. For further analysis we verified the domain ams3.digitaloceanspaces.com resolves to this endpoint IP address.

Regarding the logout/disconnect process initiated from Cyberduck Client application. The Cyberduck Client is disconnected by clicking the disconnect bottom on Cyberduck GUI this process is presented in Appendix A. On analyzing the memory dump taken at this time as a part of live acquisition 2 from our work flow diagram. In terms of network analysis, it's just disconnecting the TCP connection and take the TCP connection status to CLOSE_WAIT means the application still open whereas all connection made by application to remote side is closed.

Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f logout_cyberduck_memdump.mem netscan



0x11fcad010	TCPv4	10.0.2.15:49205	104.25.219.21:443	CLOSED	2300	Wireshark.exe
0x11fcad440	TCPv4	10.0.2.15:49218	5.101.110.225:443	CLOSED	2208	Cyberduck.exe
0x11fcaeae0	TCPv4	-:49208	23.52.27.27:80	CLOSED	908	svchost.exe
0x11fcb0cf0	TCPv4	10.0.2.15:49193	5.101.110.225:443	CLOSE_WAIT	2208	Cyberduck.exe
0x11fd609d0	TCPv4	10.0.2.15:49211	85.253.0.130:80	CLOSED	908	svchost.exe
0x11fd70a90	TCPv4	10.0.2.15:49213	10.0.2.15:80	CLOSED	260	svchost.exe

Figure 11. TCP connection CLOSED and CLOSE_WAIT for DO Space

4.3.4.2 IBM COS

Command

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f IBM_COS_memdump.mem netscan

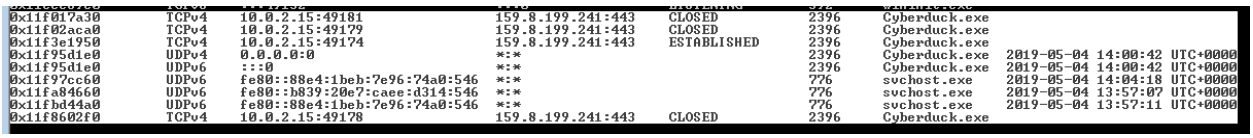


Figure 12. List of Network Connection with IBM COS

Like in the analysis of DO spaces we figured out the remote cloud storage endpoint domain s3.ams03.cloud-object-storage.appdomain.cloud resolves to the IP address 159.8.199.241 which have TCP connection status Established and Closed.

For the logout/disconnect process initiated from Cyberduck Client application similar result was traced like in DO Spaces above section i.e all TCP connection is on CLOSED and CLOSED_WAIT state.

4.3.4.3 Rackspace Cloud Files

Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f rackspace-memdump.mem netscan

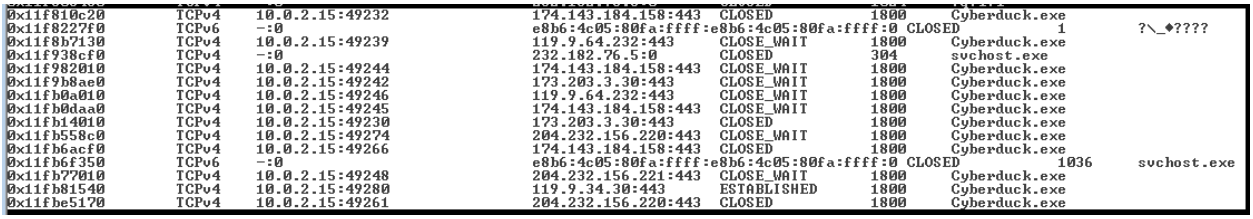


Figure 13. List of Network Connection with Rackspace Cloud Files.

Here in this analysis we have the similar output as in above section i.e Cyberduck Client Application is in the process of communication with multiple IP address on port 443. We have listed all IP address below:

- 174.143.184.158

- 119.9.64.232
- 173.203.3.30
- 204.232.156.220
- 204.232.156.221

Regarding these ip addresses on making query within www.whois.com [59] it is confirmed all ip addresses belongs to Rackspace hosting services. A sample query result for single ip address is presented in below Figure 14.

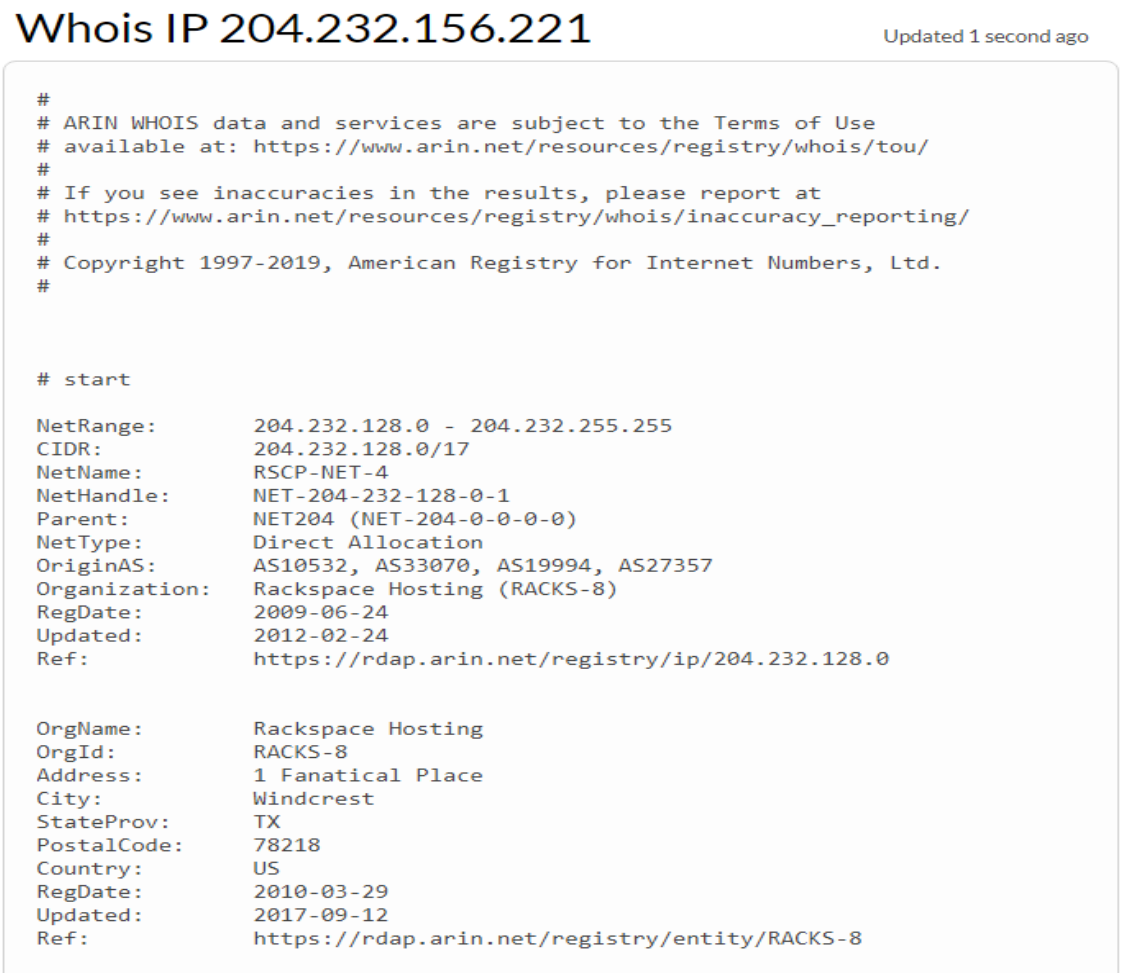


Figure 14. Results for query for ip address from whois.com

For the logout/disconnect process initiated from Cyberduck Client application similar result was traced like in DO Spaces and IBM COS in above section i.e all TCP connection is on CLOSED and CLOSED_WAIT state.

4.3.5 Hive List

We manage to list all major registry hives with the help of volatility command hivelist/

Command

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f DO_memdump.mem hivelist

Figure 15. Hive list DO Memory Dump

4.3.6 MFT Parser

We manage to have a look around the MFT parser command with volatility to trace files and directory that is forensic interest. The output from the command was redirected to a file mftparser.txt and started searching with keyword Cyberduck following facts related to Cyberduck client application was revealed.

4.3.6.1 Cyberduck History Folder

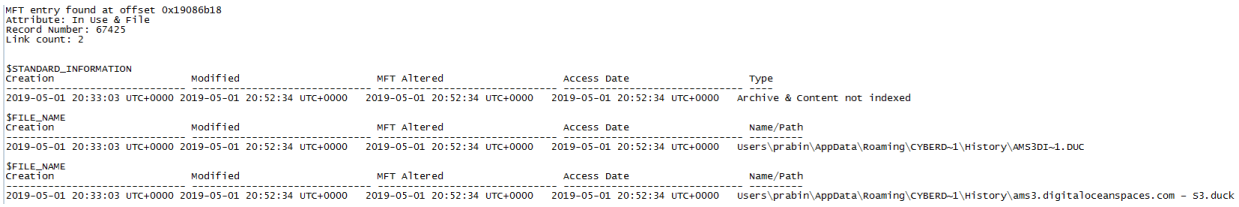
Command:

C:\Users\prabin\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win7SP1x64 -f Digital_ocean.mem mftparser > mftparser.txt

Ongoing through the file mftparser.txt and searching with key word Cyberduck we found the endpoint domain name "**ams3.digitaloceanspaces.com**" associated with file name under path Users\prabin\AppData\Roaming\CYBERD~1\History\ams3.digitaloceanspaces.com. We will

discuss about this path in detail in section disk analysis. From below Figure 16. we have collected the following detail:

- Creation Date: 2019-05-01 (Time: 20:33:03)
- Modified Date: 2019-05-01 (Time: 20:52:34)
- Access Date: 2019-05-01 (Time: 20:52:34)



```
MFT entry found at offset 0x19086b18
Attribute: In Use & File
Record Number: 67425
Link count: 2

$STANDARD_INFORMATION
Creation                  Modified                  MFT Altered               Access Date               Type
------------------------- ------------------------- ------------------------- ------------------------- ----
2019-05-01 20:33:03 UTC+0000 2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   Archive & Content not indexed

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------- ------------------------- ------------------------- ------------------------- ---------
2019-05-01 20:33:03 UTC+0000 2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   Users\prabin\AppData\Roaming\CYBERD~1\History\AMS3DI~1.DUC

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------- ------------------------- ------------------------- ------------------------- ---------
2019-05-01 20:33:03 UTC+0000 2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   2019-05-01 20:52:34 UTC+0000   Users\prabin\AppData\Roaming\CYBERD~1\History\ams3.digitaloceanspaces.com ~ S3.duck
```

Figure 16. Cyberduck History folder

4.3.6.2 Transfer logs file

On further searching with keyword on mftparser.txt we found transfer log file on path Users\prabin\AppData\Roaming\Cyberduck\Transfers\49c5db82-9922-40df-8bf8-9eef8745d190.cyberducktransfer. We will discuss about this directory in detail in section disk analysis. On going through the mftparser.txt following artifacts was collected for transfer logs file.

- Creation Date: 2019-05-01 (Time: 20:58:08)
- Modified Date: 2019-05-01 (Time: 20:58:08)
- Access Date: 2019-05-01 (Time: 20:58:08)

4.3.6.3 Installation Log

Further searching with keyword Cyberduck we found the log file associated with the installation log for Cyberduck client application. Ongoing through the mftparser.txt following artifacts was collected installation log file.

- Creation Date: 2019-05-01 (Time: 18:18:34)
- Modified Date: 2019-05-01 (Time: 18:18:34)
- Access Date: 2019-05-01 (Time: 18:18:34)

4.4. FTK imager Volatile Memory

The Memory dump image mounted with the help of FTK imager and the image was verified by within FTK imager with the help of verify image functionality verify within image FTK imager. It simply calculated the MD5sum hash of memory dump image and we verified it with one we computed during live acquisition of physical memory which stored in Table 2. Once the hash matched we proceed our analysis with the string-based analysis to collect multiple forensic artifacts regarding the volatile memory forensic which we have discussed in below sections.

4.4.1 Installation Path

To find the installation search was made with keyword Cyberduck on FTK Imager just by doing ctrl+f or can be done by right click and search through within FTK imager GUI and inserting the search string of your choice. We manage to trace the installation location for Cyberduck as shown in Figure 17 below.

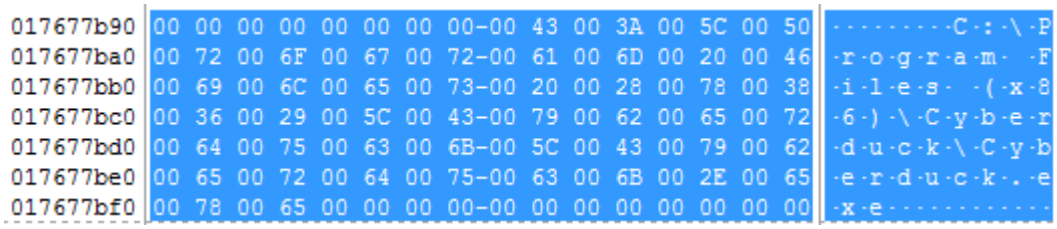


Figure 17. Cyberduck Installation Path FTK Imager Memory Dump Analysis

Which we already discussed in installation artifact section for Cyberduck. On our continuous search with keyword Cyberduck we manage to locate path. *C:\Users\prabin\AppData\Roaming*

4.4.2 GET and PUT

On searching with domain name, it was found that Cyberduck Client uses GET method to send any request from the remote cloud storage like object information and PUT to upload the files to the remote cloud storage unit.

4.5. Digital Ocean Spaces

In this section all, potential forensic artifacts which is associated with the local machine with setup for Cyberduck client application to reach DO Spaces is discussed.

4.5.1. Username and Password

By searching with string username as keyword in FTK imager it was managed to find the remote username and remote hostname that is used to connect to the remote DO spaces as listed below.

- Remote Username: N4I5QCSJ5EF3ZZLTS5L5
- Hostname: ams3.digitaloceanspaces.com

Now, search was continued based on hostname (ams3.digitaloceanspaces.com), and further trace following detail related to local system as well remote DO spaces were obtained.

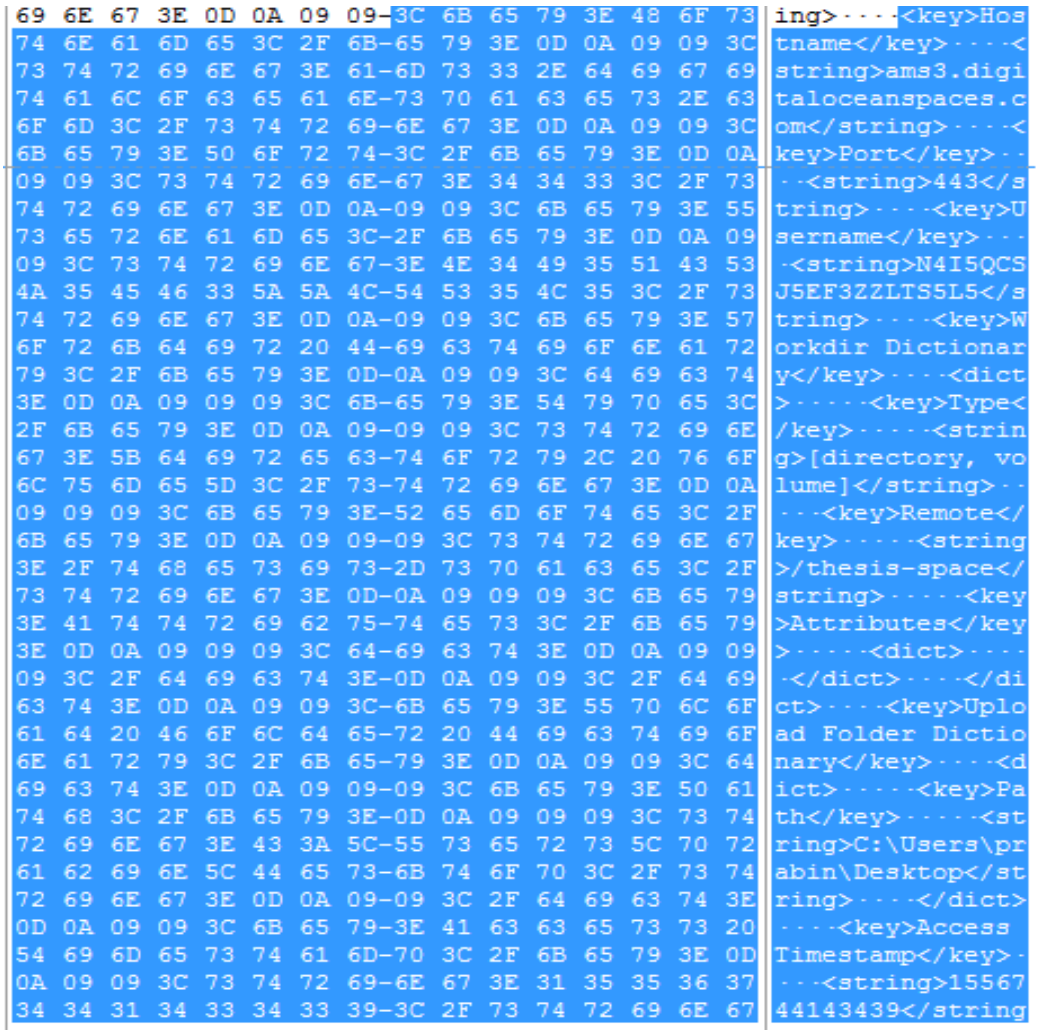


Figure 18. XML File detail about the Cyberduck Client and DO Spaces

Following is the list of the few important artifacts which are forensically important whereas it was further managed to generate the entire xml file by copying only text from FTK imager presented within Appendix B.

- Local Directory: C:\Users\prabin\Desktop\thesis_files
- Protocol: s3
- Hostname: ams3.digitaloceanspaces.com
- Port: 443
- Username: N4I5QCSJ5EF3ZZLTS5L5
- Remote: thesis-space
- Size: 4846075
- Action: Mirror

Further searching with domain name, managed to capture the Access key (Secret key provided by DO to access the Spaces).

Secret = 5xTrPqdYsLU1Iu2/z6VXKKy7VlzZkuBM6uf8h12+Utk

As per DO spaces API documentation this is AWS V4 signature type [68].

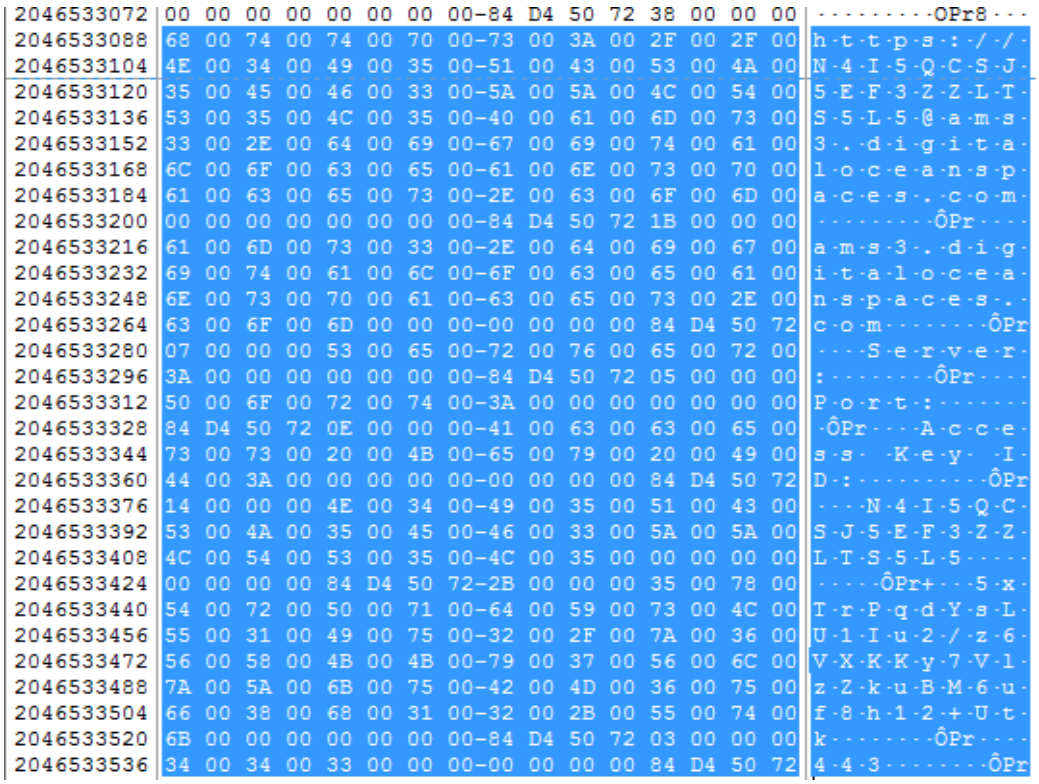


Figure 19. Digital Ocean Spaces Hostname, Username and Secret key

4.5.2 Remote File/Folder Metadata

In above section, the name of remote cloud storage unit (thesis-space) was found. To find the artifacts related to server-side string search with keyword thesis-space were continued, and tracing the location related to files and folder in local directory as well in remote Cloud storage unit were managed. While searching with key work thesis-space it was found the space creation date the time zone is based on Amsterdam (GMT +2) 2019-04-07 (9:34:16Pm) as Amsterdam data center was selected during space creation.

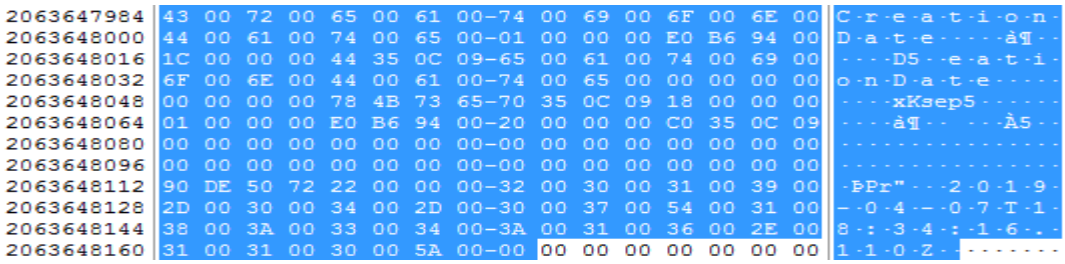


Figure 20. DO space Creation date

On further searching with key word name of DO Space some important evidences related to metadata of files and folder on remote DO space were traced. In this case, these files and folder

are located under thesis-space in DO Cloud Storage. Further it was managed to capture these data when it was browsed thesis-space via Cyberduck client application as it was simply listing the content of Bucket. These artifacts were verified with the DO official documentation for Digital Ocean Spaces API [60]. Given below is list of files with detail information about the metadata related to individual's objects inside DO spaces (thesis-space).

Below mention are list of files that were uploaded with their respective metadata.

I. sample1_zip.zip

- Is Truncated: False
- Max Uploads: 1000

Contents:

a) key: sample1_zip.zip

b) Last Modified: 2019-05-01T20:58:31.469

c) Etag (md5sum): da87f50c9267efec0d30620b517f194a

d) Size: 4640671

e) Storage Class: STANDARD

Owner

i. ID: 293026

ii. DisplayName: 293026

II. sample2_docx.docx

- Is Truncated: False
- Max Uploads: 1000

Contents:

a) key: sample2_docx.docx

a) Last Modified: 2019-05-01T20:58:14.206Z

a) Etag (md5sum): 30ac5dcee7208b6fa6febf10708a4df9

b) Size: 4098

c) Storage Class: STANDARD

Owner

i. ID: 293026

ii. DisplayName: 293026

III. sample3_picture.jpeg

- Is Truncated: False
- Max Uploads: 1000

Contents:

a) key: sample3_picture.jpeg

a) Last Modified: 2019-05-01T20:58:13.179

a) Etag (md5sum): 490fbaff4ba2301d35c96b1eb2167efa

b) Size: 11241

c) Storage Class: STANDARD

Owner

i. ID: 293026

ii. DisplayName: 293026

IV. sample4.txt

- Is Truncated: False
- Max Uploads: 1000

Contents:

a) key: sample4.txt

a) Last Modified: 019-05-01T20:58:13.373Z

a) Etag (md5sum): b71bfde4dbeb91919b91bb89e27409d4

b) Size: 8969

c) Storage Class: STANDARD

Owner

i. ID: 293026

ii. DisplayName: 293026

Sample output from FTK Imager when we copy Text only for single file as below.

<.B.u.c.k.e.t.>.t.h.e.s.i.s.-
.s.p.a.c.e.<./.B.u.c.k.e.t.>.<.M.a.x.U.p.l.o.a.d.s.>.1.0.0.0.<./.M.a.x.U.p.l.o.a.d.s.>.<.I.s.T.r.u.n.c.
a.t.e.d.>.f.a.l.s.e.<./.I.s.T.r.u.n.c.a.t.e.d.>.<./.L.i.s.t.M.u.l.t.i.p.a.r.t.U.p.l.o.a.d.s.R.e.s.u.l.t.>.s.a.m
.p.l.e.1._.z.i.p...z.i.p.<./.K.e.y.>.<.L.a.s.t.M.o.d.i.f.i.e.d.>.2.0.1.9.-.0.5.-
.0.1.T.2.0.:.5.8.:.3.1...4.6.9.Z.<./.L.a.s.t.M.o.d.i.f.i.e.d.>.<.E.T.a.g.>.&.q.u.o.t.;.d.a.8.7.f.5.0.c.9.2
.6.7.e.f.e.c.0.d.3.0.6.2.0.b.5.1.7.f.1.9.4.a.&.q.u.o.t.;.<./.E.T.a.g.>.<.S.i.z.e.>.4.6.4.0.6.7.1.<./.S.i.z
.e.>.<.S.t.o.r.a.g.e.C.l.a.s.s.>.S.T.A.N.D.A.R.D.<./.S.t.o.r.a.g.e.C.l.a.s.s.>.<.O.w.n.e.r.>.<.I.D.>.
2.9.3.0.2.6.<./.I.D.>.<.D.i.s.p.l.a.y.N.a.m.e.>.2.9.3.0.2.6.<./.D.i.s.p.l.a.y.N.a.m.e.>.<./.O.w.n.e.r.
>.<./.C.o.n.t.e.n.t.s.>.

These are four test files users in local system which was synchronized to remote DO Space (thesis-space) via Cyberduck client application. Later it was verified with the md5sum of these files with one that was taken before files were transferred which are presented in Table 1. for DO spaces.

4.5.3 Deleted File

To collect the artifacts related to the deletion of file. On Cyberduck GUI interface we listed all objects inside the DO spaces right click and deleted the file sample4.txt and memory dump was taken as part of Live acquisition 2. On making search based on endpoint domain, the delete request was traced as shown in below Figure 21.

- Request Type: DELETE
- Date: 07 May 2019 17:46:40
- Host: ams3.digitaloceanspaces.com
- Filename: sample4.txt

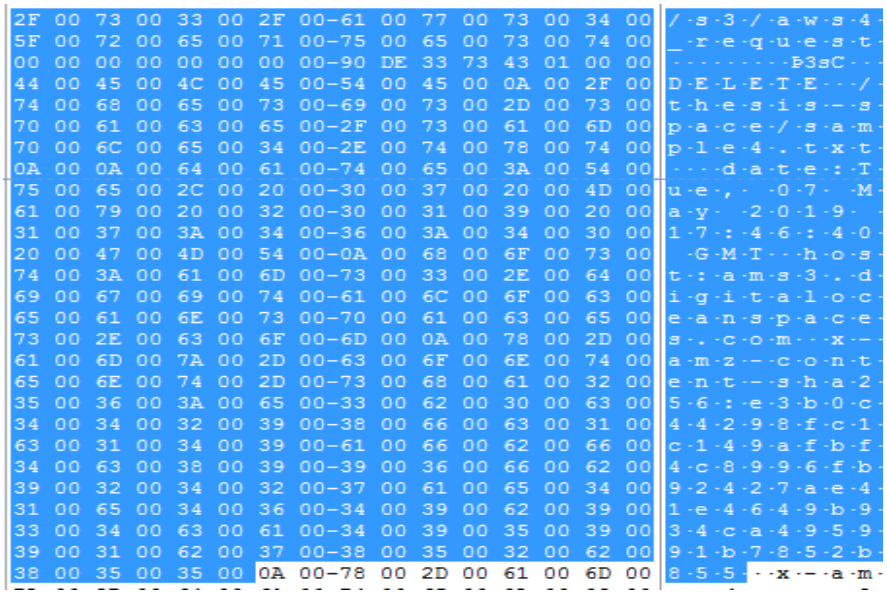


Figure 21. Object Delete Request DO Space

4.6. IBM COS

In this section, the same procedure was followed as in above section to analyze the volatile memory dump that is associated the client machine in which it was configured the Cyberduck client application for IBM COS. Given below is list of files with detail information about the metadata related to individual's objects inside thesis-cos, which came as the output of command list bucket when tried to browse to the content of ibm-cos via Cyberduck Client applocation on local machine.

4.6.1. Username and Password

In this section to capture the username and password i.e access key and secret access key that is provided during configuration of IBM COS with cloud service prodder web console. String based search was conducted within FTK Imager with keyword username and managed to capture the login credentials for IBM COS as shown in below Figure 22 and Figure 23. Thus, found username and password details as follows:

- Username (access_key_id): 6409e863e6ed4227937fe0f5915a5983
- Password(secret_access_key): a1cfc6a7008180d78f12d1b1cec9618da67c52f1210c9a66

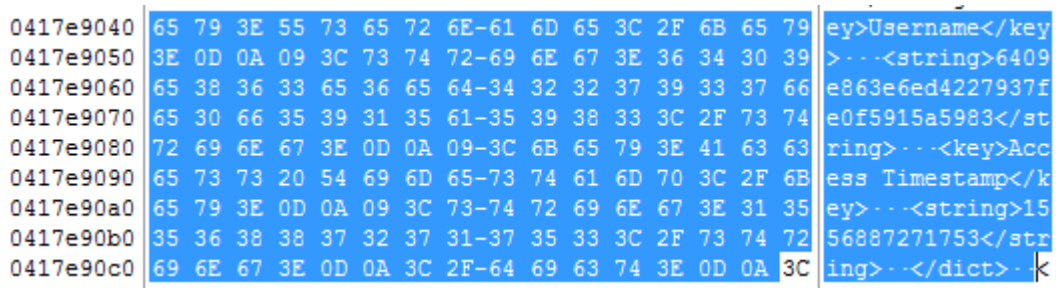


Figure 22. Username for IBM COS Endpoint

Figure 23. Username (access_key_id), password (secrect_access_key) and endpoint

4.6.2. Remote File/Folder Metadata

Tracing the creation date for IBM COS was done by making the string search based on endpoint domain name s3.ams03.cloud-object-storage.appdomain.cloud . The creation date for IBM COS in our case it is named as thesis-cos created data is 05.03.2019 2:43:53 PM. Like in above section the local directory path C:\Users\prabin\Desktop\thesis_files to the sync folder with remote cloud storage were found.

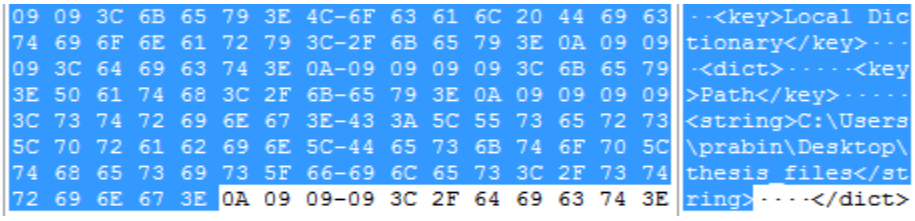


Figure 24. Path to the local Directory for synchronize directory

Similarly, like in above section by searching with remote IBM COS name that is created to store the files and folder or object in this case it was named as thesis-cos. On searching with keyword thesis-cos it was found with some important artifacts related to the metadata of objects that is stored in remote cloud storage unit.

Below mention are list of files that were uploaded with their respective metadata which is verified with md5sum within in Table 3.

I. sample1-IBM-COS-TXT

- Is Truncated: False
- Max Uploads: 1000

  Contents:

  a) key: sample1-IBM-COS-TXT

  b) Last Modified: 2019-05-04T14:01:11.716

  c) Etag (md5sum): a9ae8a1317db155001a234335af7b8ca

  d) Size: 13874

e) Storage Class: STANDARD

Owner

iii. ID: 7af24f66-1dda-4c54-a388-a1054e153618

iv. DisplayName: 7af24f66-1dda-4c54-a388-a1054e153618

II. sample2_IBM_COS.jpeg

- Is Truncated: False
- Max Uploads: 1000

Contents:

b) key: sample2_IBM_COS.jpeg

a) Last Modified: 2019-05-04T14.01:14.435

b) Etag (md5sum): D0c93df1d49ce699d3542059f9801cf6

b) Size: 7171

c) Storage Class: STANDARD

Owner

iii. ID: 7af24f66-1dda-4c54-a388-a1054e153618

iv. DisplayName: 7af24f66-1dda-4c54-a388-a1054e153618

III. Sample3-IBM-COS.docx

- Is Truncated: False
- Max Uploads: 1000

Contents:

b) key: Sample3-IBM-COS.docx

a) Last Modified: 2019-05-04T14:01:23.143

b) Etag (md5sum): 188204e37bd808f0a01f5984abc36515

b) Size: 2760957

c) Storage Class: STANDARD

Owner

iii. ID: 7af24f66-1dda-4c54-a388-a1054e153618

iv. DisplayName: 7af24f66-1dda-4c54-a388-a1054e153618

IV. sample4-IBM-COS-pdf.pdf

- Is Truncated: False
- Max Uploads: 1000

Contents:

b) key: sample4-IBM-COS-pdf.pdf

a) Last Modified: 019-05-01T20:58:13.373Z

b) Etag (md5sum): f195d7d2ab7f403a1a87164124b170fe

b) Size: 190023

c) Storage Class: STANDARD

Owner

iii. ID: 7af24f66-1dda-4c54-a388-a1054e153618

iv. DisplayName: 7af24f66-1dda-4c54-a388-a1054e153618

The has and the filename for each file mentioned above with the hash value we have in Table 3.

4.6.3 Deleted File

To collect the artifacts related to the deletion of file. On Cyberduck GUI interface we listed all objects inside the DO spaces right click and deleted the file sample4-IBM-COS-pdf.pdf and

memory dump was taken. We manage to take the separate memory dump to capture the artifacts related to deletion of files. In given below Figure 25 we traced the Delete request sent from Cyberduck Client.

- Request Type: DELETE
- Date: Fri 10 May 2019 12:41:47 GMT
- Host: s3.ams03.cloud-object-storage.appdomain.cloud
- Filename: sample4-IBM-COS-pdf.pdf

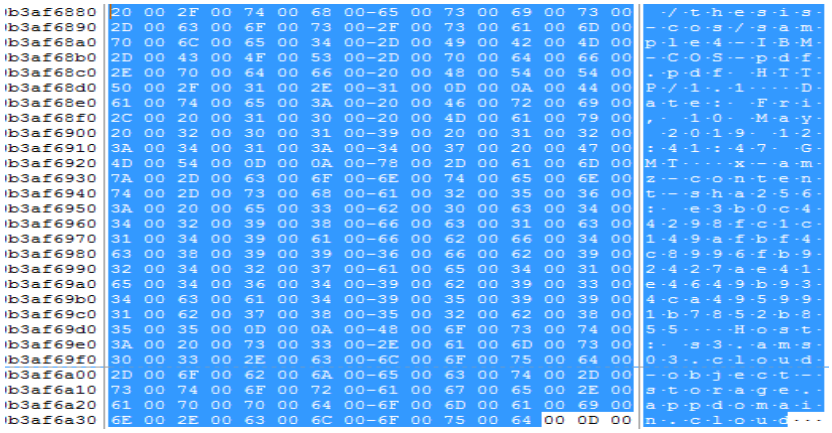


Figure 25. Delete Request IBM COS

4.7. Rackspace Cloud Files

In this section, the same procedure was followed that was conducted for IBM COS and DO Spaces to capture the essential forensic artifacts that which is residing in volatile memory

4.7.1 Username and Password

As compare to the DO spaces and IBM COS Rackspace cloud files have different settings. As it doesn't provide distinct username to access the storage unit whereas username remains the same as you have for cloud console login and password is API key generated for individual users. Also, in terms of Cyberduck client application it has in build profile for Rackspace cloud files we have presented the xml file example in Appendix C. Whereas, for DO Space and IBM COS S3 is chosen as both are constructed for s3 compatibility. In this section string search was conducted with

keyword username like in above sections and successful in tracing the username and API key that is used for Rackspace cloud files.

- Username: prabin
- Api Key: 04e214f490ed41abb66eb4c96bb3bd65

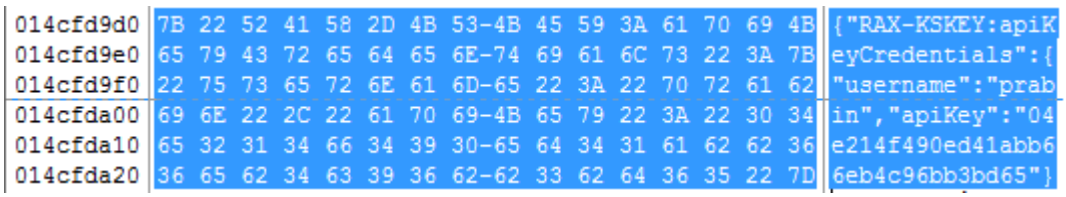


Figure 26. Rackspace Cloud Files username and API Key

4.7.2 Remote File/Folder Metadata

Search based on string identity.api.rackspacecloud.com were conducted and found that the xml file providing the basic information about the remote/file location. Some major artifacts found are presented below:

- Remote Container: rackspace-cloud-object-thesis
- Region: IAD [61]
- Local Path: C:\Users\prabin\Desktop\thesis-rackspace

Now search was conducted with string rackspace-cloud-object-thesis and during this search it was found that some important artifacts related to the metadata of objects that is stored in remote cloud storage unit as listed below:

I. sample1-Rackspace-txt.TXT

- Container Name: rackspace-cloud-object-thesis
- Object Name: sample1-Rackspace-txt.TXT
- Hash: 2008597e3a51acdde7114249f9d1c28
- Size: 23528 bytes

- Content Type: text/plain
- Last Modified: 2019-05-05T15:32:42.903460

II. sample2-Rackspace-pdf.pdf

- Container Name: rackspace-cloud-object-thesis
- Object Name: sample2-Rackspace-pdf.pdf
- Hash: 3159999a42fbb864e72025b180b3723d
- Size: 2594237 bytes
- Content Type: application/pdf
- Last Modified: 2019-05-05T15:32:42.963480

III. sample3-Rackspace-jpg.jpg

- Container Name: rackspace-cloud-object-thesis
- Object Name: sample3-Rackspace-jpg.jpg
- Hash: f8001686e624353f792a394e07263644
- Size: 4098257 bytes
- Content Type: image/jpeg
- Last Modified: 2019-05-05T15:33:05.976130

IV. sample4-Rackspace.tar.gz

- Container Name: rackspace-cloud-object-thesis
- Object Name: ample4-Rackspace.tar.gz
- Hash: b55e09c19c8f10125e8137f08d560145
- Size: 329978 bytes

- Content Type: application/octet-stream
- Last Modified: 2019-05-05T15:33:05.976130

The sample xml file related to above presented data for single file is as below.

<containername="rackspace-cloud-object-thesis"><object><name>sample1-Rackspace-txt.TXT</name><hash>12008597e3a51acdde7114249f9d1c28</hash><bytes>23528</bytes><content_type>text/plain</content_type><last_modified>2019-05-05T15:32:42.903460</last_modified></object>

All above presented data with Rackspace Cloud files metadata is verified with the Rackspace API documentation [62] and the all md5sum for the respective files is verified within the Table 2.

4.7.3 Deleted Files

We could not find any type forensic artifacts related to the deleted files from the dump analysis of volatile memory from the client configure local machine. As per the forensic framework we are using to conduct our research this can be done as iterative process. So, we again went to the collection state and regenerated the similar setup and live acquisition was done. On our second attempt also, we could not capture any trace of deleted files form memory.

4.8 Physical Disk Analysis

Entire hard disk from each local machine was acquired with the help FTK imager installed in external drive in E01 format. Disk acquisition was done in two phases first one was done after the installation of client application including user activities like login to remote cloud storage unit and successful file transfer. Second phase was done after deleting the file from local sync folder and user logout. Thus, md5sum was computed for phases of disk acquisition which can be found in Appendix D. Further analysis was done by adding on the image as evidence in an FTK Imager following windows forensics analysis steps followed by other forensic academic studies like [63].

4.8.1 Windows Registry

Windows registry is rich source of information to trace changes made to the system due to the activities like installation, uninstallation and many more user activities that will make changes on

system which are logged in registry. Such made changes to the system can be presented as one of the major evidences during the time of forensic examination. Analysis started with exporting the major windows registry hives via FTK Imager. The exported registry is than analyzed with FTK Registry viewer to collect the further evidences.

4.8.2 HKEY_LOCAL_MACHINE\Software

To export the Registry hives in FTK imager the evidence image is loaded, the path for this hive in image is windows/system32/config select the SOFTWARE hives and right clicks and export to the files. Such exported hive is saved and md5sum is taken to maintain the integrity.

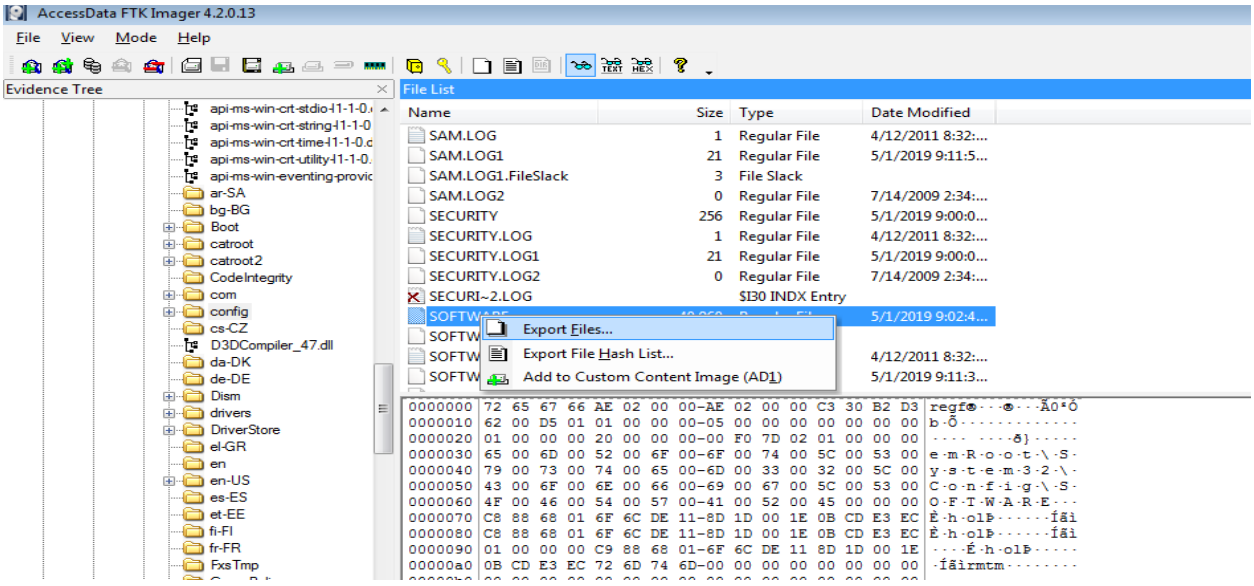


Figure 27. Export Registry Hive Software

The exported hive is loaded into registry viewer for further analysis. On path SOFTWARE/Wow6432Node/Cyberduck it was found the application installation date (Last Written Time: 4/19/2019 T6:44:32 UTC), Application Description, AppicationIcon (Installation Path) and ApplicationName .

- Installation Date: 4/19/2019 T6:44:32 UTC
- Application Description: Libre FTP, SFTP, WebDAV, S3 and OPENStack Swift browser for mac AND Windows
- Application Icon: C:\Program Files(x86)\Cyberduck\Cyberduck.exe

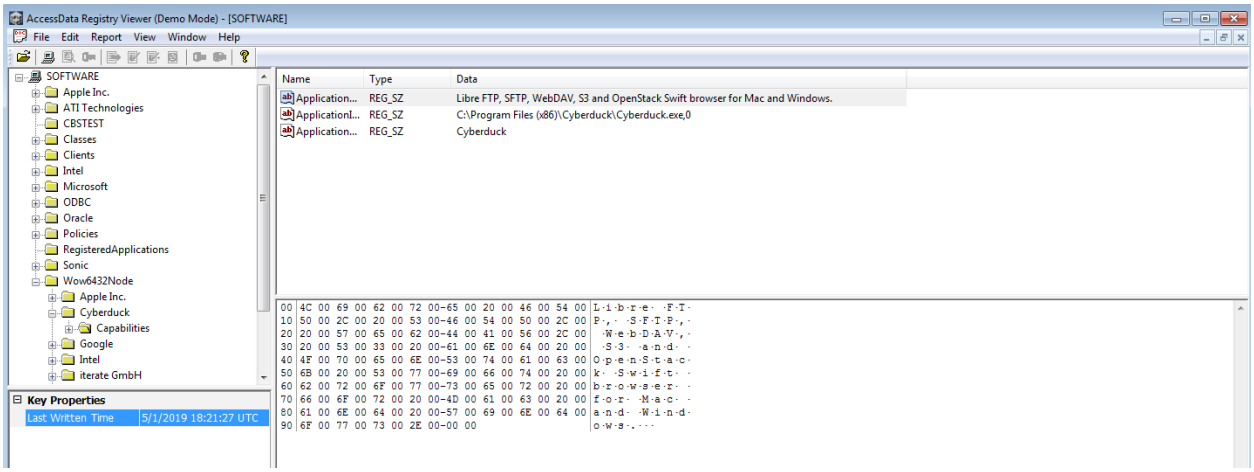


Figure 28. Cyberduck Installation Date

Likewise on path software\Microsoft\windows\currentversion\installer\folders to the location of the installation path (C:\Program Files(x86)\Cyberduck\ and C:\Program Files(x86)\Cyberduck\profile) for Cyberduck Client application on windows 7 OS were found. Both location holds the significant value in terms of Installation artifact.

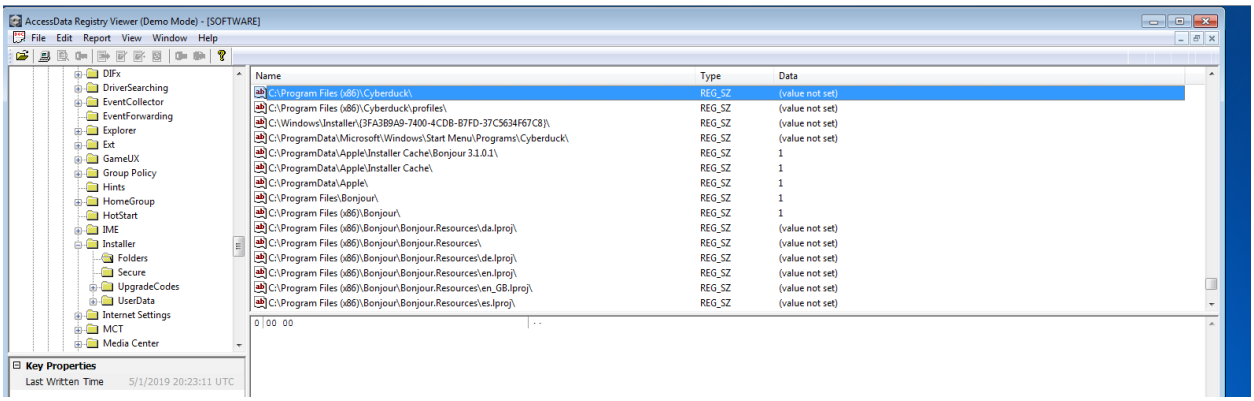


Figure 29. Cyberduck Installation Path

4.8.3 HKEY_CURRENT_USER (NTUSER.DAT)

To export the Registry hives in FTK imager the evidence image is loaded, the path for this hive in image is windows/system32/Users/prabin (active user in the system) select the NTUSER.DAT hives and right click and export to the files and md5sum is taken. The exported NTUSER.DAT is open with FTK registry viewer for further analysis. It was found the path to the Cyberduck Client application NTUSER.DAT/Software/iterate GmBH and the last written time is the date Cyberduck

was executed in the system. Here in the path NTUSER.DAT/Software/iterate GmBH, iterate GmBH belongs to the name of the of Cyberduck development company [64].

4.8.4 Sync Folder

From volatile memory analysis we figured out the path to the synchronize folder is on path Users\prabin\Desktop\thesis_files which is sync with the Digital Ocean spaces (thesis-space). Verifying the content C:\Users\prabin\Desktop\thesis_files via FTK Imager. On navigating the to the path FTK imager it was found all four files with date of modification.

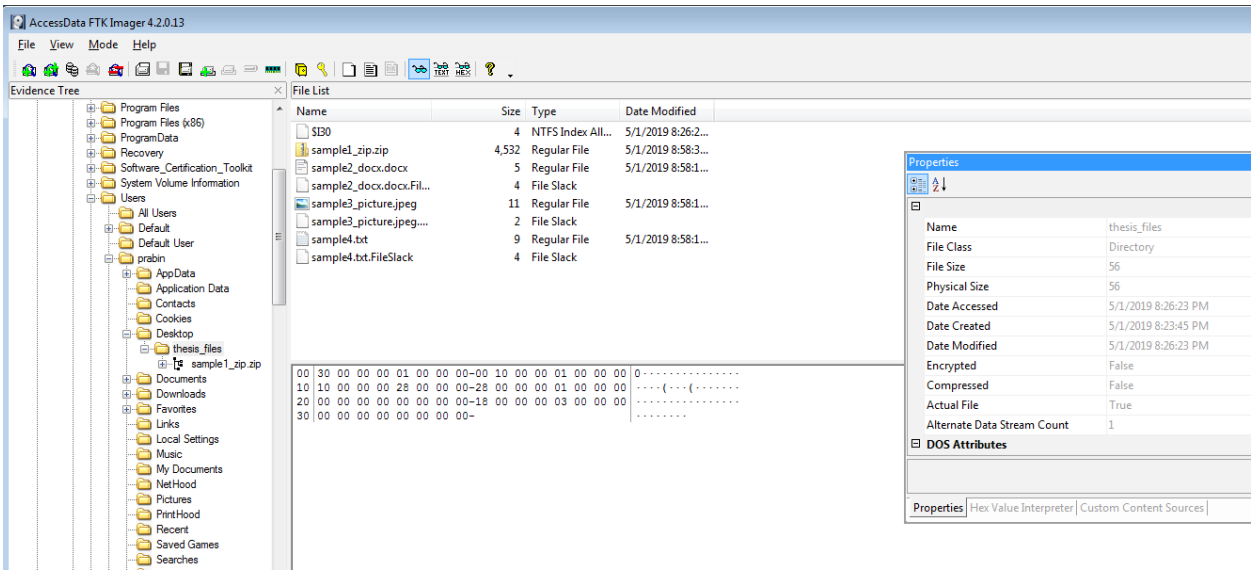


Figure 30. Path to the sync Folder

4.8.5 Installation Path

During the analysis of registry, it was found the installation path C:\Program Files(x86)\Cyberduck and C:\Program Files(x86)\profile. On analyzing both path via FTK imager, it traced multiple files related to the Cyberduck Installation and inside the profile folder, and thus found the profiles for multiple cloud storage, which are supported by Cyberduck Client application.

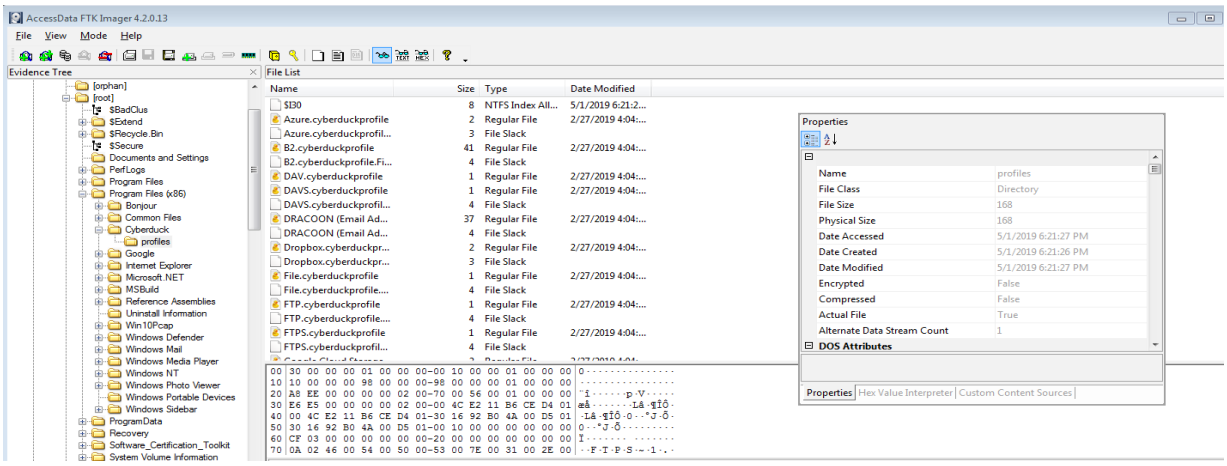


Figure 31. List of Cyberduck Supported Profiles

4.8.6 Lnk Files

These files are also known as shortcut and leads to the other mail path of files in the system. Its path normally depends on how the application is installed in the system, for most application it asked for user permission to placed shortcut it in the Desktop and some of the application automatically does it. In this case, Cyberduck does not ask place the shortcut on desktop but still it was managed to trace the shortcut link on path C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Cyberduck and when browsed this path via FTK imager found the file Cyberduck.lnk file with its date of modification.

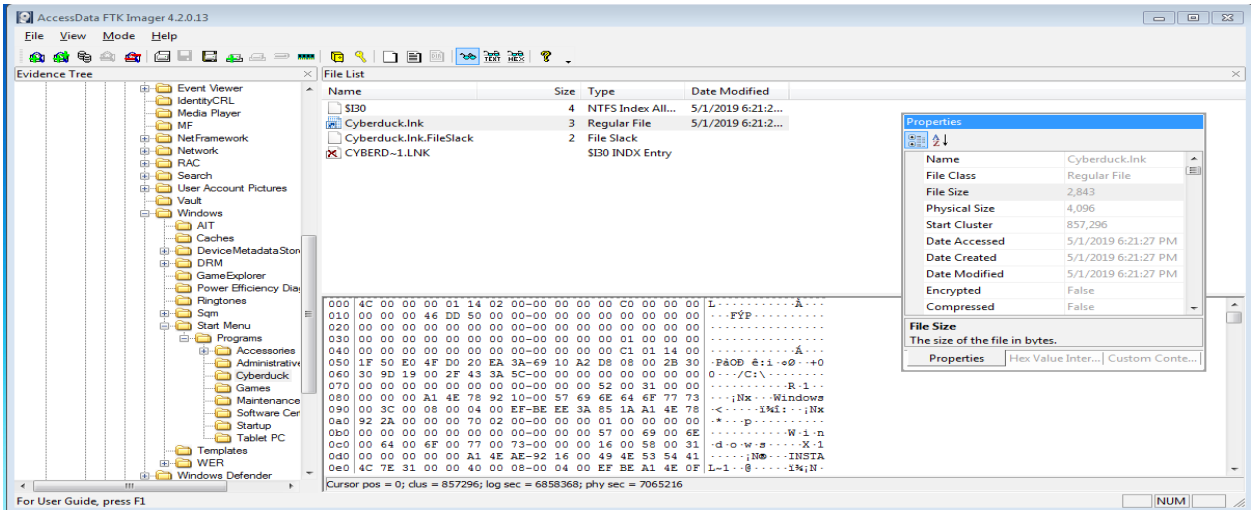


Figure 32. Lnk file path

4.8.7 Jump List

The path for for Jump List files are under user profile path and normally it is C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations and associated files are *.automaticDestinations-ms. It was managed so as to extract the Jump List via FTK Imager and loaded to the Jump List Viewer.

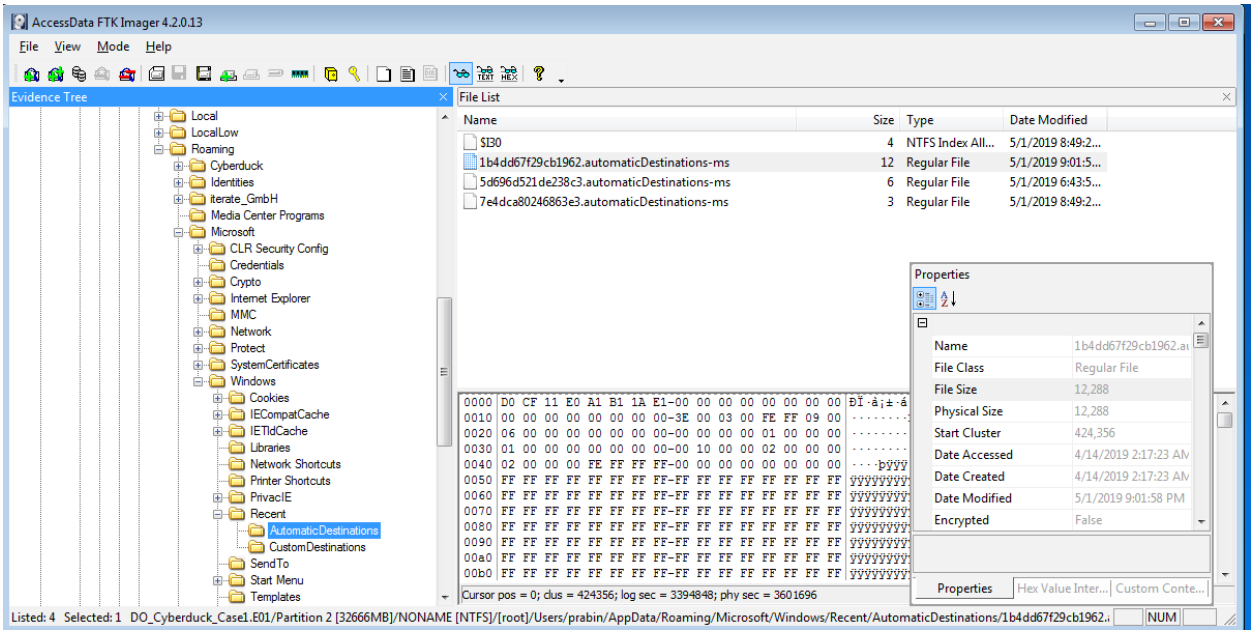


Figure 32. Jump list export path

4.8.8 AppData

To analyze the appdata the path C:\Users\prabin\AppData\Roaming\Cyberduck was navigated via FTK Imager. On this path found following files and brief info about each files and folder which are listed below [65]

- Bookmarks: Contains the bookmarks for multiple connection for ease of connectivity.
- cyberduck.log: log files, it seems to quite unclear, but we can see only error log.
- History: History of last successful communication between client and server
- Profiles: Any saved profile by Cyberduck client in our case Digital Ocean Space.
- Sessions: Session detail of present time

- Transfers: Detail of every transfer file/folder (Upload, Download and Synchronize).

On inspecting the files inside Transfer this folder details like path of folder on local machine were found that is synchronize with cloud storage, remote cloud storage detail in this case have Digital Ocean Space, Access Timestamp, Bandwidth, Sync Type, Remote Server Hostname, Port, Total Size of files transferred and Username. Taking the particular case of DO spaces below presented is the sample file that is associated with the transfer file log of client machine configured with client application to reach DO spaces.

- Local Directory: C:\Users\prabin\Desktop\thesis_files
- Protocol: s3
- Hostname: ams3.digitaloceanspaces.com
- Port: 443
- Username: N4I5QCSJ5EF3ZZLTS5L5
- Remote : thesis-space
- Size: 4846075
- Action: Mirror

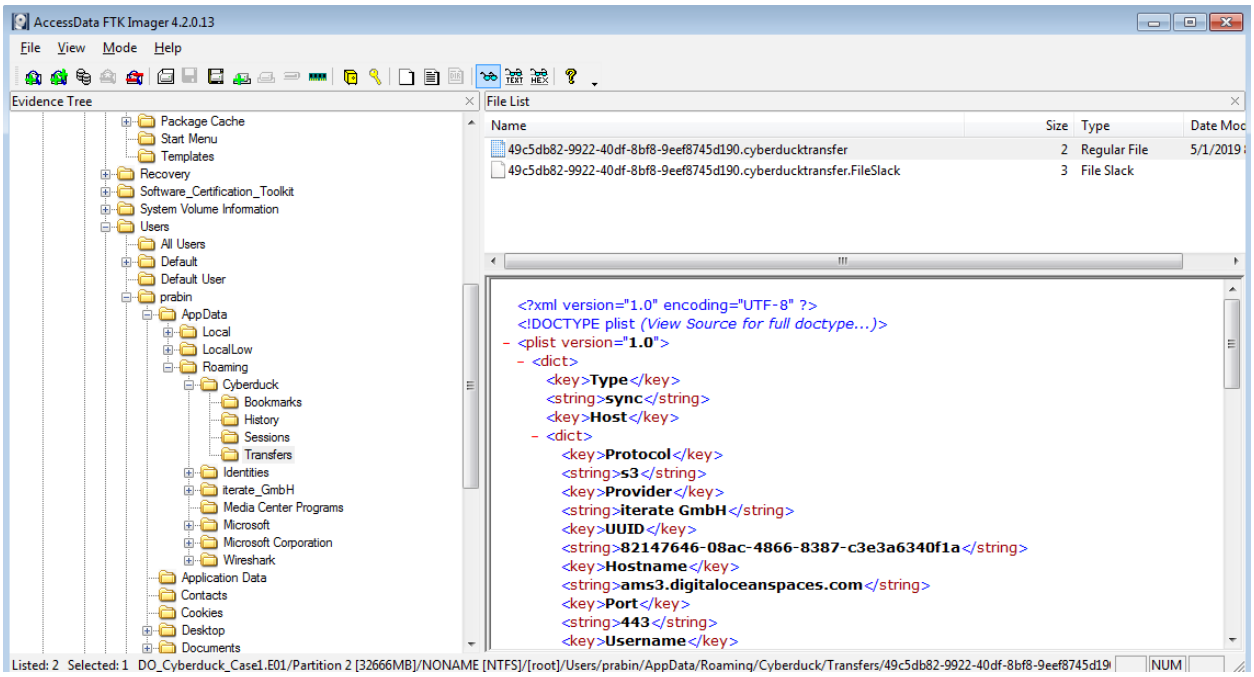


Figure 34. Transfer configuration File location for Cyberduck Client

The file containing the content of transfer logs is in XML format considering the typical case of DO Spaces as below:

<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE plist (View Source for full doctype...)>

- <plist version="1.0">

- <dict>

<key>Type</key>

<string>sync</string>

<key>Host</key>

- <dict>

<key>Protocol</key>

<string>s3</string>

<key>Provider</key>

<string>iterate GmbH</string>

<key>UUID</key>

<string>82147646-08ac-4866-8387-c3e3a6340f1a</string>

<key>Hostname</key>

<string>ams3.digitaloceanspaces.com</string>

<key>Port</key>

<string>443</string>

<key>Username</key>

<string>N4I5QCSJ5EF3ZZLTS5L5</string>

<key>Workdir Dictionary</key>

- <dict>

<key>Type</key>

<string>[directory, volume]</string>

<key>Remote</key>

<string>/thesis-space</string>

<key>Attributes</key>

<dict />

</dict>

<key>Upload Folder Dictionary</key>

- <dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop</string>

</dict>

<key>Access Timestamp</key>

<string>1556744356122</string>

</dict>

<key>Items</key>

- <array>

- <dict>

<key>Remote</key>

- <dict>

<key>Type</key>

<string>[directory, volume]</string>

<key>Remote</key>

<string>/thesis-space</string>

<key>Attributes</key>

<dict />

</dict>

<key>Local Dictionary</key>

- <dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis_files</string>

</dict>

</dict>

</array>

<key>UUID</key>

<string>49c5db82-9922-40df-8bf8-9eef8745d190</string>

<key>Size</key>

<string>4664979</string>

<key>Current</key>

<string>4664979</string>

<key>Timestamp</key>

<string>1556744362559</string>

<key>Bandwidth</key>

<string>-1.0</string>

<key>Action</key>

<string>mirror</string>

</dict>

</plist>

4.8.9 User Config

With the help of FTK imager we managed to find the user configuration file on path Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164\user.config.

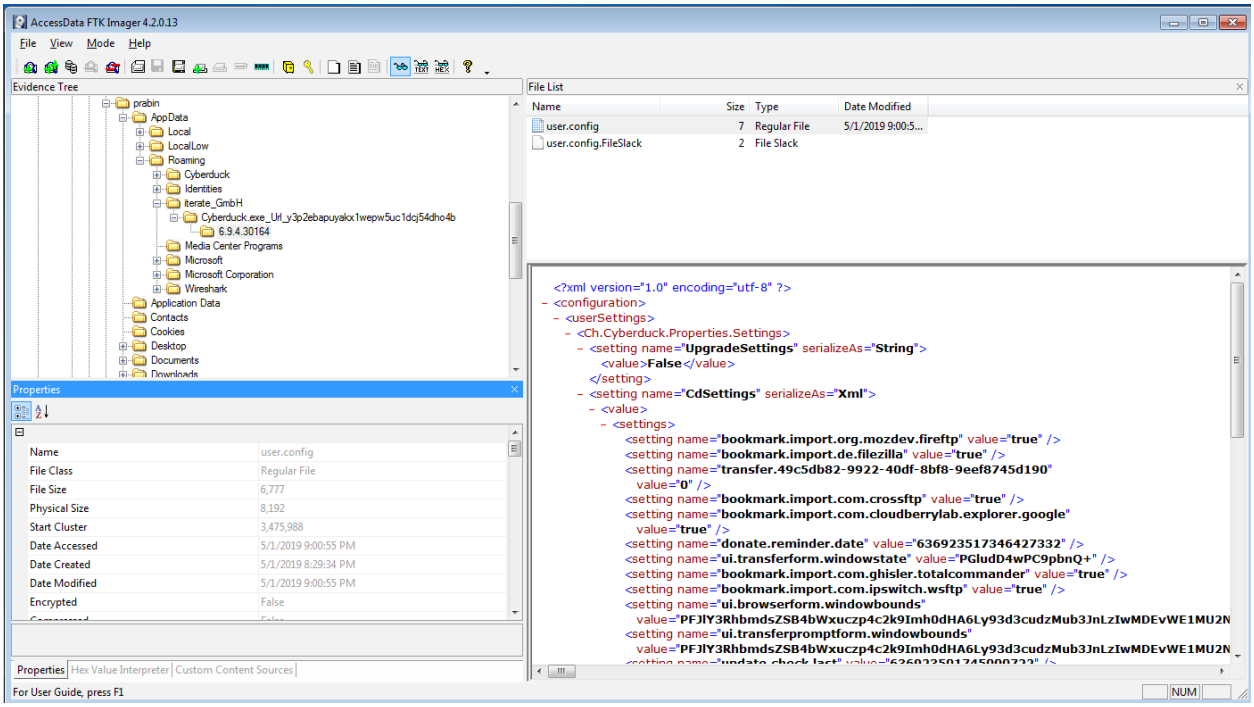
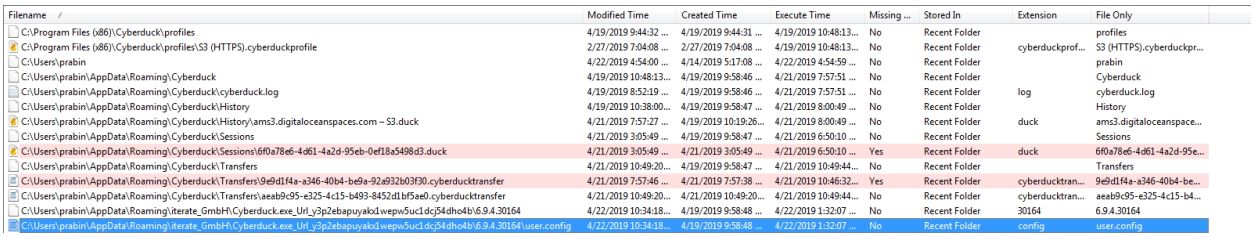


Figure 3. user-config file location

4.8.10 Recent Files

Extracting the recent files with FTK Imager from path C:\Users\username\AppData\Roaming\Microsoft\Recent and then the exported file was opened with recent files application for further analysis. The path to the files that is been accessed or executed by the user whereas; the focus was on Cyberduck so only those recent files that were accessed by user, which is related to cyberduck client Application only were presented.



Filename	Modified Time	Created Time	Execute Time	Missing ...	Stored In	Extension	File Only
C:\Program Files (x86)\Cyberduck\profiles	4/19/2019 9:44:32 ...	4/19/2019 9:44:31 ...	4/19/2019 10:48:13...	No	Recent Folder		profiles
C:\Program Files (x86)\Cyberduck\profiles\S3 (HTTPS).cyberduckprofile	2/27/2019 7:04:08 ...	2/27/2019 7:04:08 ...	4/19/2019 10:48:13...	No	Recent Folder	cyberduckprof...	S3 (HTTPS).cyberduckpr...
C:\Users\prabin	4/22/2019 4:54:00 ...	4/14/2019 5:17:08 ...	4/22/2019 4:54:59 ...	No	Recent Folder		prabin
C:\Users\prabin\AppData\Roaming\Cyberduck	4/19/2019 10:48:13...	4/19/2019 9:58:46 ...	4/21/2019 7:57:51 ...	No	Recent Folder		Cyberduck
C:\Users\prabin\AppData\Roaming\Cyberduck\cyberduck.log	4/19/2019 8:52:19 ...	4/19/2019 9:58:46 ...	4/21/2019 7:57:51 ...	No	Recent Folder	log	cyberduck.log
C:\Users\prabin\AppData\Roaming\Cyberduck\History	4/19/2019 10:38:00...	4/19/2019 9:58:47 ...	4/21/2019 8:00:49 ...	No	Recent Folder		History
C:\Users\prabin\AppData\Roaming\Cyberduck\History\ams3.digitaloceanspaces.com – S3.duck	4/21/2019 7:57:27 ...	4/19/2019 10:19:26...	4/21/2019 8:00:49 ...	No	Recent Folder	duck	ams3.digitaloceanspace...
C:\Users\prabin\AppData\Roaming\Cyberduck\Sessions	4/21/2019 3:05:49 ...	4/19/2019 9:58:47 ...	4/21/2019 6:50:10 ...	No	Recent Folder		Sessions
C:\Users\prabin\AppData\Roaming\Cyberduck\Sessions\6f0a78e6-4d61-4a2d-95eb-0ef18a5498d3.duck	4/21/2019 3:05:49 ...	4/21/2019 3:05:49 ...	4/21/2019 6:50:10 ...	Yes	Recent Folder	duck	6f0a78e6-4d61-4a2d-95e...
C:\Users\prabin\AppData\Roaming\Cyberduck\Transfers	4/21/2019 10:49:20...	4/19/2019 9:58:47 ...	4/21/2019 10:49:44...	No	Recent Folder		Transfers
C:\Users\prabin\AppData\Roaming\Cyberduck\Transfers\9e9d1f4a-a346-40b4-be9a-92a932b03f30.cyberducktransfer	4/21/2019 7:57:46 ...	4/21/2019 7:57:38 ...	4/21/2019 10:46:32...	Yes	Recent Folder	cyberducktran...	9e9d1f4a-a346-40b4-be...
C:\Users\prabin\AppData\Roaming\Cyberduck\Transfers\aeab9c95-e325-4c15-b493-8452d1bf5ae0.cyberducktransfer	4/21/2019 10:49:20...	4/21/2019 10:49:20...	4/21/2019 10:49:44...	No	Recent Folder	cyberducktran...	aeab9c95-e325-4c15-b4...
C:\Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164	4/22/2019 10:34:18...	4/19/2019 9:58:48 ...	4/22/2019 1:32:07 ...	No	Recent Folder	30164	6.9.4.30164
C:\Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164\user.config	4/22/2019 10:34:18...	4/19/2019 9:58:48 ...	4/22/2019 1:32:07 ...	No	Recent Folder	config	user.config

Figure 36. Recent File View

4.8.11 MFT

MFT record was extracted with FTK Imager and was passed to mft2scv for further analysis. The output from the mft3csv tool was saved and opened with Microsoft windows excel. To trace the files and folder that reference to Cyberduck client application search was done with keyword Cyberduck. On this search process location of files and folder that refer to Cyberduck client application was found as presented in below Figure 37.

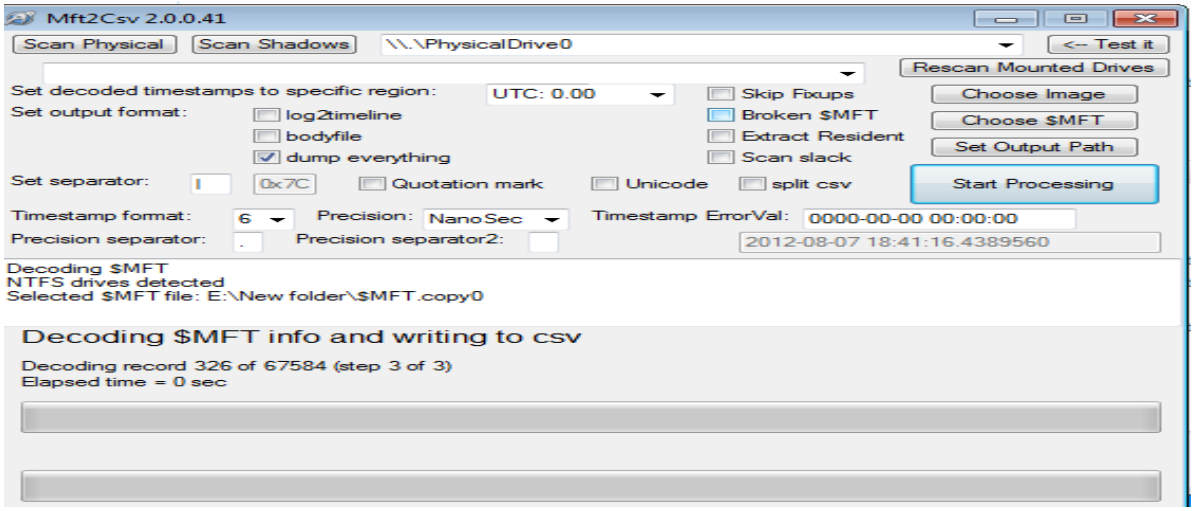


Figure 37. MFT to CSV Conversion process

Figure 40. List of files from MFT record that related to the Cyberduck

4.8.12 Event Logs

Logs plays a vital role during forensic evidence collection the path for the logs in windows 7 OS is C:\Windows\System32\Winevt\Logs we managed to Extract all event logs via FTK imager for further analysis.

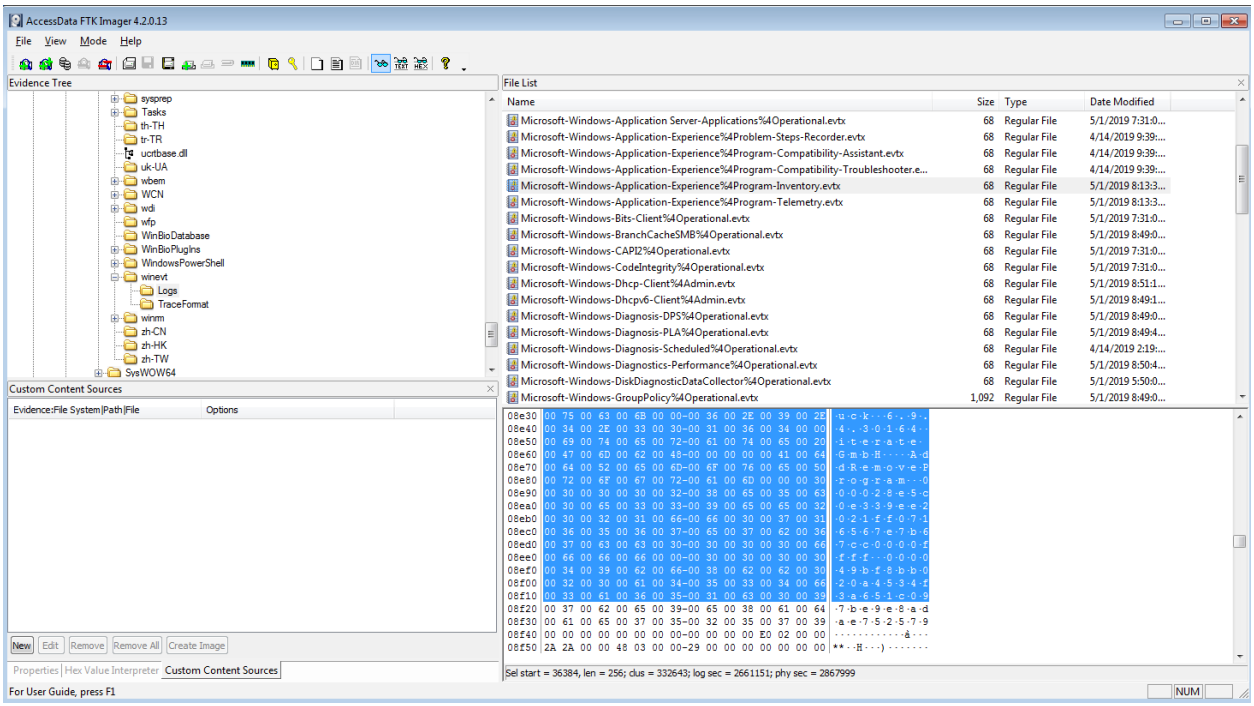


Figure 39. Cyberduck Client Application sample log

4.8.13 Deleted Files

To analyze the deleted files from the disk we used the Autopsy tool. We took the disk image that we got from Disk acquisition 2 and added as new case in Autopsy to trace and recovered the files deleted by user in local machine. In this section we will recover the sample file that we have deleted from each local machine associated individual client application setup for cloud storage.

4.8.13.1 Digital Ocean Space

In this case we have deleted the sample4.txt file from the local sync directory. We loaded the DO disk image acquired from Disk Acquisition 2 from our workflow diagram. On Autopsy GUI navigate to view>File Types>Deleted files here we can see the list of files that is deleted on right hand side of Autopsy GUI. On searching manually by scrolling the down the list of deleted files we found deleted sample4.txt as shown in below Figure 42. The brief metadata about the deleted file is as below Table 7:

Name	/img_DO_Space_Image_file_deleted_1.1.E01/vol_vol3/Users/prabin/Desktop/thesis_files/sample4.txt
Type	File System
MIME Type	text/plain
Size	8969
Modified	2019-05-01 23:58:13 EEST
Accessed	2019-05-01 23:26:23 EEST
Created	2019-05-01 23:26:23 EEST
Changed	2019-05-09 22:11:45 EEST
MD5	b71bfde4dbeb91919b91bb89e27409d4

Table 7. DO Spaces Metadata Deleted File

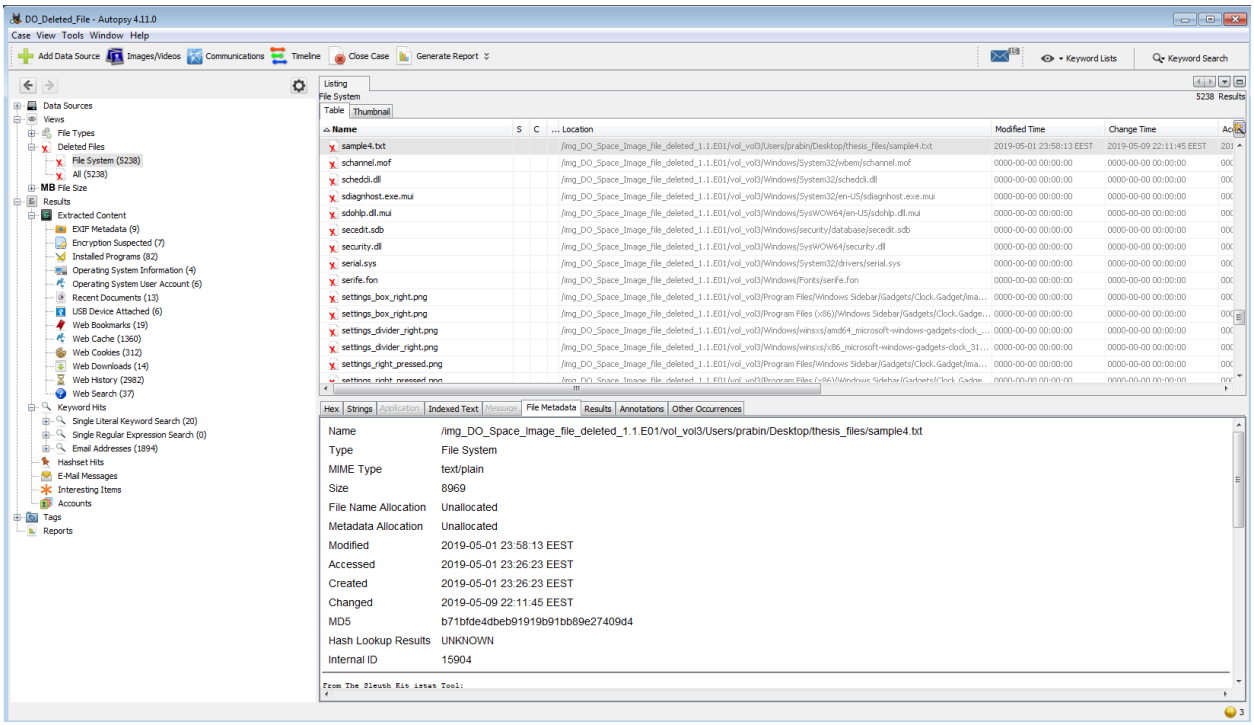


Figure 40. Metadata of deleted file

To Extract the files right click the file and extract as shown in below Figure 43. After extracting the file, we computed md5sum of retrieved it matches the with one that we computed before deletion of file as presented in above Table 7. Which assured the integrity of file is preserved?

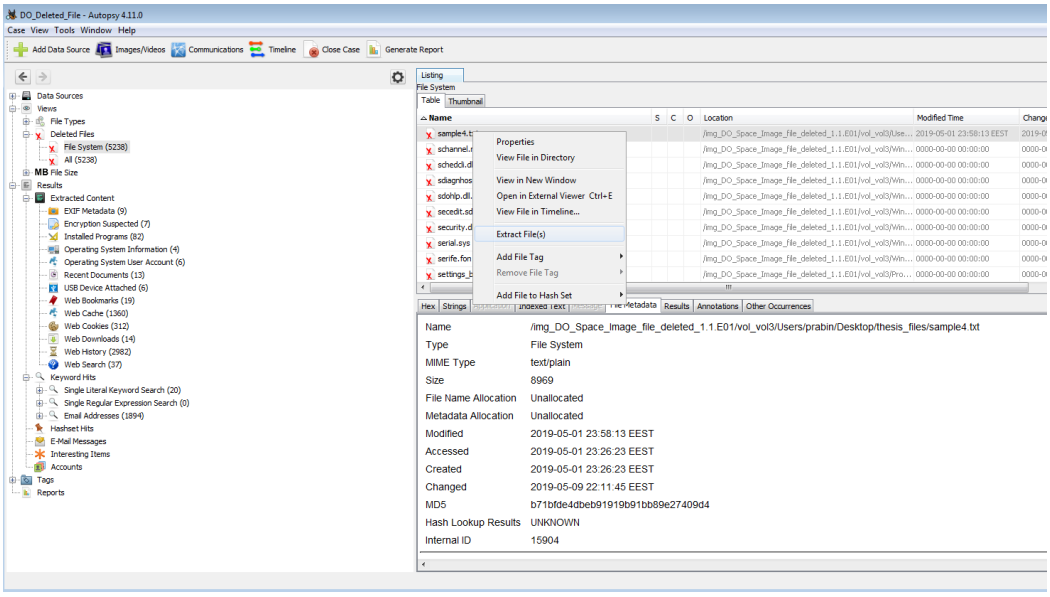


Figure 43. Autopsy Extract Deleted file

4.8.13.2 IBM COS

Following the similar process that we used for retrieving the deleted files with Autopsy we simply retrieved the deleted file sample4-IBM-COS-pdf.pdf. Thus, extracted file md5sum is computed and verified with the existing one we have in Table 3. To ensure the integrity of data. Below Table 8. shows the detail we attained from Autopsy.

Name	/img_IBM_DISK_Analysis_DeletedFile2.1.E01/vol_vol3/Users/prabin/Desktop/ibm-cos/sample4-IBM-COS-pdf.pdf
Type	File System
MIME Type	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size	2760957
Modified	2019-05-04 17:01:23 EEST
Accessed	2019-05-03 16:28:11 EEST
Created	2019-05-03 16:28:11 EEST
Changed	2019-05-07 01:21:32 EEST
MD5	f195d7d2ab7f403a1a87164124b170fe

Table 8. IBM COS Metadata Deleted File

4.8.13.3 Rackspace Cloud files

Following the similar process that we used for retrieving the deleted files with Autopsy we simply retrieved the deleted file sample4-Rackspace.tar.gz thus extracted file md5sum is computed and verified with the existing one we have in Table 2. To ensure the integrity of data. Below Table 9 shows the detail we attained from Autopsy.

Name	/img_Rackspace_delete_file_analysis_3.1.E01/vol_vol3/ Users/prabin/Desktop/ibm-cos/ sample4-Rackspace.tar.gz
Type	File System
MIME Type	application/octet-stream
Size	766
Modified	2019-05-07 01:17:11 EEST
Accessed	2019-05-07 01:17:11 EEST
Created	2019-05-07 01:17:11 EEST
Changed	2019-05-07 01:17:11 EEST
MD5	B55e09c19c8f10125e8137f08d560145

Table 9. Rackspace Metadata Deleted File

5. Result and Evaluation

In this section analysis of the result to obtain the evidence that is of forensic interest by using the proven tools and technology are done. Various forensics artifacts were collected as part of installation artifacts, network forensic, live forensic and static analysis of disk. Development of the real time scenario to capture the evidence in multiple state of user activities like installation of client application, login to remote cloud storage service provider, data transfer between local machine to remote cloud storage, collection of forensic evidence from volatile memory, and windows forensic. Analysis are divided into two parts as Cyberduck Client Installation Artifacts and Remote Storage Analysis artifacts.

5.1 Cyberduck Client Installation Artifacts

This section deals with major artifacts that is collected regarding the installation of Cyberduck client application on windows 7 OS. Study about installation artifacts is based on file system, registry, services and drivers are done. Using tool windows system state analyzer and windows system state monitor, installation was found, and result is presented in below Table 10.

	Installation Artifacts	**Volatile Memory Analysis**	**Static Analysis**
Installation Path	C:\Program Files (x86)\Cyberduck	PROGRA~2\CYBERD~1\Cyberduck.exe	Program Files(x86)\Cyberduck\
Setup Log	C:\Users\prabin\AppData\Local\Temp\Cyberduck_20190501211834_001_Setup.log	Users\prabin\AppData\Local\Temp\Cyberduck_20190501211834_001_Setup.log	Users\prabin\AppData\Local\Temp\Cyberduck_20190501211834_001_Setup.log
History Log Path	C:\Users\prabin\AppData\Roaming\Cyberduck\History	Users\prabin\AppData\Roaming\Cyberduck\History	C:\Users\prabin\AppData\Roaming\Cyberduck\History

Transfer Log Path	C:\Users\prabin\AppData\Roaming\Cyberduck\Transfers	Users\prabin\AppData\Roaming\Cyberduck\Transfers	Users\prabin\AppData\Roaming\Cyberduck\Transfers
Bookmarks	C:\Users\prabin\AppData\Roaming\Cyberduck\Bookmarks	Users\prabin\AppData\Roaming\Cyberduck\Bookmarks	Users\prabin\AppData\Roaming\Cyberduck\Bookmarks
Cyberduck Log File	C:\Users\prabin\AppData\Roaming\Cyberduck\cyberduck.log	Users\prabin\AppData\Roaming\Cyberduck\cyberduck.log	Users\prabin\AppData\Roaming\Cyberduck\cyberduck.logUser
User Config	C:\Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164\user.config	Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164\user.config	Users\prabin\AppData\Roaming\iterate_GmbH\Cyberduck.exe_Url_y3p2ebapuyakx1wepw5uc1dcj54dho4b\6.9.4.30164\user.config
Link Files	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Cyberduck	ProgramData\Microsoft\Windows\Start Menu\Programs\Cyberduck	ProgramData\Microsoft\Windows\Start Menu\Programs\Cyberduck
Events Log	C:\Windows\System32\winevt\Logs\Application.evtx	Windows\System32\winevt\Logs\Application.evtx	Windows\System32\winevt\Logs\Application.evtx

Table 10. Cyberduck Primary Installation Artifacts

5.2 Digital Ocean Spaces Artifacts

	Network Forensic	**Live Forensic**	**Static Analysis**
Username (Access Key)		N4I5QCSJ5EF3ZZLTS5L5	
Password (Secret)		5xTrPqdYsLU1Iu2/z6VXKKy7VlzZkuBM6uf8h12+Utk	
IP Address	5.101.110.225	5.101.110.225	
Server (Domain Name)	ams3.digitaloceanspaces.com	ams3.digitaloceanspaces.com	Users\prabin\AppData\Roaming\Cyberduck\History\ams3.digitaloceanspaces.com – S3. duck
Local Path		Users\prabin\Desktop\thesis_files	Users\prabin\Desktop\thesis_files
Remote Path		/thesis-space	Users\prabin\AppData\Roaming\Cyberduck\Transfers\49c5db82-9922-40df-8bf8-9eef8745d190.cyberducktransfer
Space Creation Date		2019-04-07T9:34:16Pm	
Remote Space Size		4846075	

Remote Space Region	ams3	ams3	ams3
Port of Connection	443	443	443
Owner ID		293026	

Table 11. Digital Ocean Spaces Primary Artifacts

5.3 IBM COS Artifacts

	Network Forensic	**Live Forensic**	**Static Analysis**
Username (Access Key)		6409e863e6ed4227937fe0f5915a5983	
Password (Secret)		a1cfc6a7008180d78f12d1b1cec9618da67c52f1210c9a66	
IP Address	159.8.199.241	159.8.199.241	
Server (Domain Name)	s3.ams03.cloud-object-storage.appdomain.cloud	s3.ams03.cloud-object-storage.appdomain.cloud	Users\prabin\AppData\Roaming\Cyberduck\History\s3.ams03.cloud-object-storage.appdomain.cloud – S3.duck
Local Path		C:\Users\prabin\Desktop\ibm-cos	Users\prabin\Desktop\ibm-cos
Remote Path		/thesis-cos	C:\Users\prabin\AppData\Roaming\Cyberduck\Transfers\77b4ca05-bb71-47b5-9408-

			616cdd3c5306.cyberduck transfer
IBM COS Creation Date		05.03.2019 2:43:53	
IBM COS Size		2972025	
Remote Space Region		ams03	ams03
Port of Connection	443	443	443
Owner ID		7af24f66-1dda-4c54-a388-a1054e153618	

Table 12. IBM COS Primary Artifacts

5.4 Rackspace Cloud Files Artifacts

	Network Forensic	**Live Forensic**	**Static Analysis**
Username (Access Key)		prabin	
Password (API Key)		04e214f490ed41abb66eb4c96bb3bd65	
IP Address	174.143.184.158, 119.9.64.232, 173.203.3.30, 204.232.156.220, 204.232.156.221	174.143.184.158, 119.9.64.232, 173.203.3.30, 204.232.156.220, 204.232.156.221	
Local Path		C:\Users\prabin\Desktop\thesis-rackspace	Users\prabin\Desktop\thesis-rackspace

Remote Path		/rackspace-cloud-object-thesis	C:\Users\prabin\AppData\Roaming\Cyberduck\History\identity.api.rackspacecloud.com – Cloud Files.duck
Cloud Files		2019-05-05T15:32:42.903460	
Cloud File Container Size		7046000	
Remote Space Region		IAD	
Port of Connection	443	443	443
Owner ID		7af24f66-1dda-4c54-a388-a1054e153618	

Table 13. Rackspace Cloud Files Primary Artifacts

From the results presented above captured some of the major artifacts from client machine perspective, which can provide the major lead to forensic researcher, academician and investigator during similar kind of research. Interims of Network Forensic captured the traffic on multiple state of user activities like upload, download and deleting of files from cloud storage unit. It was found the traffic encrypted with TLSV1.2, still managed to capture the endpoints for cloud storage, IP address, protocol used and ports of communication.

5.6 Result Analysis Table

This section deals with the tabular representation of all the major artifacts that is captured during this research study. Table 14. below present the artifacts that were collected in different states of analysis.

Artifacts	DO Spaces			IBM COS			Rackspace Cloud Files		
	Network	Volatile Memory	Disk Analysis	Network	Volatile Memory	Disk Analysis	Network	Volatile Memory	Disk Analysis
Username		□	□		□	□		□	□
Password		□			□			□	
Remote Endpoint	□	□	□	□	□	□	□	□	□
IP Address	□	□		□	□		□	□	
Local Path		□	□		□	□		□	□
Remote Path		□	□		□	□		□	□
Remote Object Storage		□			□			□	

Creation date									
Remote Object Storage Name		□	□		□	□		□	□
Remote Object Name		□	□		□	□		□	□
Remote Object md5sum		□			□			□	
Remote Object Creation Date		□			□				
Remote Object Modified Date		□			□			□	
Remote Object Size		□			□			□	

Remote Object Content Type								□	
Remote Object Delete Date		□			□			□	
Cloud Storage Region		□	□		□	□		□	□
Cloud Storage Owner ID		□			□			□	
Cyberduck Transfer Log		□	□		□	□		□	□
Cyberduck History Log		□	□		□	□		□	□
Cyberduck Log		□	□		□	□		□	□

Cyberduck Connection Profile		□	□		□	□		□	□
Local Deleted File		□	□		□	□		□	□

Table 14. Result Analysis

5.7 Discussion

In this section we will have the brief discussion about our findings based on methodology we developed and compare contrast about the evidence collected for all three-object based cloud storage. We mentioned in above section during this study we are following the cloud forensic framework introduce by Martini and Choo [50] which is one of the widely accepted frameworks by many researchers and investigators. The potential sources of evidences in our case Windows 7 OS, 32GB hard disk, 4GB RAM hosted on VirtualBox 6.0 and cloud storage services DO Spaces, Rackspace cloud files and IBM COS. We collected all potential data sources as a part of evidence collection and md5sum was computing to insure the integrity of collected data sources and the evidences sources collected are network dump with Wireshark, live acquisition with FTK Imager and disk acquisition with FTK Imager. During analysis phase we managed to analyze all data sources considering the keywords like username, password, remote endpoint domain name, remote object storage name, client application name, and cloud service providers name.

The methodology presented in this research study is based on following headings we will briefly discuss about our findings for individual cloud storage providers specially in the case of Network forensic, Live Acquisition and Disk analysis whereas Installation artifacts completely related with Cyberduck client application.

- Installation Artifacts

- Network Forensic
- Live Acquisition
- Disk Analysis

During the analysis of installation artifacts, the major artifacts we have collected is based in changes in registry, filesystem, services and drivers. During this step we identified the artifacts related to the Cyberduck client installation like installation log, installation path, changes in files and folder, changes in registry, Cyberduck config path and changes in services we have provided this detail in above section within Table 1. We have discussed about installation artifact in detail during the windows forensic section.

We analyzed the network dump captured via Wireshark for all three-cloud storage unit. As the traffic is encrypted with TLSv1.2 and no traces to http connection. The major capture was endpoint domain name and IP address

Cloud Service Provider	**Endpoint Domain Name**	**IP Address**
Digital Ocean Spaces	ams3.digitaloceanspaces.com	5.101.110.225
IBM COS	s3.ams03.cloud-object-storage.appdomain.cloud	159.8.199.241
Rackspace Cloud Files	identity.api.rackspacecloud.com	166.78.226.217

Table 15. Cloud Storage providers endpoint domain name and IP Address

The memory dumps acquired from all three individual windows 7 OS machine associated with individual cloud service providers in our simulation environment was analyzed with the help of FTK Imager and the findings are presented in the Table 11, Table 12 and Table 13 in above section. In comparison to DO Space and IBM COS we found the Rackspace cloud files output is bit different in terms of capturing the meta data of remote object it also gives the object content type means more information about the object whereas this metadata content type is not available for DO Spaces and IBM COS. Similarly, during analysis of network via volatility forensic framework tool we found Cyberduck client application TCP connection state is established with more than

one IP addresses whereas DO spaces and IBO COS was having connection to a single remote endpoint IP address. On our query made to each IP addresses with whois.com [59] and the sample output is presented in Figure 14 shows each IP address belongs to the Rackspace hosting.

On further analysis for the deleted file details via FTK imager we could not trace anything from memory dump associated with Rackspace cloud files client machine. Whereas with remaining two other client machine we traced the DELETE request sent to remote cloud storage with timestamp. During this phase of our analysis we found there no significant difference found between DO Space and IBM COS operations. The major difference found between DO Space and IBM COS with respect to Rackspace cloud files is the way API call is made from the client application. As, Rackspace Cloud files API is implemented using RESTful web service interface whereas, both DO Spaces and IBM COS uses an implementation of S3 API.

During disk analysis most of the analysis was made with respect to the windows forensic dealing with installation artifacts and other user activities related to Cyberduck client application. In terms of Cyberduck client application operation we managed to trace the jump list, Cyberduck Installation log, Cyberduck installation path, Cyberduck file transfer log, Cyberduck history log etc. On the second phase of disk analysis we managed to retrieve the deleted files by user with the help of Autopsy tool. We have presented the retrieved information for each sample file in Table 6. Table 7. and Table 8. As we discussed in above section 4.3.4 Network Connections during the time of logout which was triggered by clicking the disconnect bottom on Cyberduck Client application. It was seen that in all three-client machine the TCP connection status to respective remote endpoints was in CLOSED and CLOSE_WAIT state.

6. Conclusion

After performing the in-depth forensic analysis of individual client machine hosted within VirtualBox with windows 7 OS. Each machine was configured with Cyberduck client application to access individual object-based cloud storage i.e. DO Spaces, IBM COS and Rackspace cloud files. In this research study we manage to develop the technical procedure to conduct the forensic investigation which will surely help forensic investigator and researchers to conduct the investigation of similar kind in real world scenario. The first step of our research was to find the evidence sources and then collection data that is of forensic interest. During collection period we performed the network dump, live acquisition, and disk acquisition in all client machine.

During volatile memory analysis we managed to trace multiple potential forensic artifacts related to remote objects in cloud storage like hash, modified date, creation data, data content type, username, password, user ID associated with cloud storage account, object storage name, object storage creation date, region associated with object storage and deletion date. Likewise, findings for local system during volatile memory analysis are network connectivity, endpoint domain name, IP address, Cyberduck client transfer log, Cyberduck log, setup files and many more artifacts related to changes in registry, filesystem which is of forensic interest.

On disk analysis forensic artifacts related to Cyberduck client application is collected from the analysis of configuration files and log generated by Cyberduck client application during installation as well as during user action like login, upload, download, delete and logout. From analyzing these files, we can identify the artifacts like username, remote endpoint for cloud storage, file transfer detail, remote object storage name, registry changes, filesystem change, meta data of files sync with remote object storage, metadata of deleted file, and recovery of deleted file.

Similarly, during the network analysis, we found all the traffic is encrypted with TLSv1.2 and the forensic artifacts collected are endpoint domain name for remote cloud storage and IP address associated with the endpoint domain name. We conclude with believe that the methodology generated here within this thesis will surely help the forensic investigator and academician to conduct study/investigation in similar kind.

Regarding the future work, further work can be done with the respective object-based cloud storage on the cloud part to collect the forensic artifacts of interest from cloud service provider point of view. Such captured artifacts can used to verify the artifacts that we captured during this study. Also, the challenges in the collection of forensic artifacts from cloud storage point of view can be interesting further study associated within this forensic investigation.

References

[1] "Dropbox, WordPress Used As Cloud Cover In New APT ..." [Online]. Available: https://www.darkreading.com/attacks-breaches/dropbox-wordpress-used-as-cloud-cover-in-new-apt-attacks/d/d-id/1140098. [Accessed: 12-May-2019].

[2] Cloud Security Alliance, "Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing," 2013. [Online]. Available: https://cloudsecurityalliance.org/research/imf/,. [Accessed: 12-May-2019].

[3] Sathishkumar Easwaramoorthy Sankar Thamburasa Guru Samy S.Bharath Bhushan1 Karrothu Aravind, "Digital Forensic Evidence Collection of Cloud Storage Data for Investigation," *IEEE*, vol. 2, no. June 2014, pp. 192–194, 2016.

[4] "DigitalOcean Launches Spaces for Easy, Scalable and Persistent Object Storage." [Online]. Available: https://www.digitalocean.com/press/releases/digitalocean-launches-spaces-for-easy-scalable-and-persistent-object-storage/. [Accessed: 12-May-2019].

[5] "Cloud Files Online Object Storage | Rackspace." [Online]. Available: https://www.rackspace.com/en-gb/cloud/files. [Accessed: 12-May-2019].

[6] "What is object storage? | IBM Cloud." [Online]. Available: https://www.ibm.com/cloud/learn/what-is-object-storage. [Accessed: 12-May-2019].

[7] "Cyberduck | Libre server and cloud storage browser for Mac and Windows with support for FTP, SFTP, WebDAV, Amazon S3, OpenStack Swift, Backblaze B2, Microsoft Azure & OneDrive, Google Drive and Dropbox." [Online]. Available: https://cyberduck.io/. [Accessed: 12-May-2019].

[8] "Cyberduck 6.2.x for Windows and macOS :: DigitalOcean Product Documentation." [Online]. Available: https://www.digitalocean.com/docs/spaces/resources/cyberduck/. [Accessed: 12-May-2019].

[9] "Transfer files with Cyberduck." [Online]. Available: https://cloud.ibm.com/docs/services/cloud-object-storage/gui?topic=cloud-object-storage-

cyberduck. [Accessed: 12-May-2019].

[10] “Configure Rackspace Cloud Files with Cyberduck.” [Online]. Available: https://support.rackspace.com/how-to/configure-rackspace-cloud-files-with-cyberduck/. [Accessed: 12-May-2019].

[11] “Deloitte hit by cyber-attack revealing clients’ secret emails | Business | The Guardian.” [Online]. Available: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails. [Accessed: 12-May-2019].

[12] “Cloud Services Being Used to Distribute Malware | CloudWedge.” [Online]. Available: https://www.cloudwedge.com/news/cloud-services-used-distribute-malware/. [Accessed: 12-May-2019].

[13] “Attackers turning to legit cloud services firms to plant malware | Computerworld.” [Online]. Available: https://www.computerworld.com/article/2484596/attackers-turning-to-legit-cloud-services-firms-to-plant-malware.html. [Accessed: 12-May-2019].

[14] “Internet Growth Statistics 1995 to 2019 - the Global Village Online.” [Online]. Available: https://www.internetworldstats.com/emarketing.htm. [Accessed: 12-May-2019].

[15] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology.”

[16] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, “Chapter 2 CLOUD FORENSICS.”

[17] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.”

[18] “The Differences Between Cloud Backup, Cloud Storage, and Cloud Sync.” [Online]. Available: https://www.backblaze.com/blog/sync-vs-backup-vs-storage/. [Accessed: 12-May-2019].

[19] “Object Storage.” [Online]. Available: https://en.wikipedia.org/wiki/Object_storage.

[Accessed: 12-May-2019].

[20] “Object Storage vs. Block Storage Services | DigitalOcean.” [Online]. Available: https://www.digitalocean.com/community/tutorials/object-storage-vs-block-storage-services. [Accessed: 12-May-2019].

[21] “Cloud Computing Architecture.” [Online]. Available: https://www.w3schools.in/cloud-computing/cloud-computing-architecture/. [Accessed: 12-May-2019].

[22] “Windows Forensics and Security | Forensic Focus - Articles.” [Online]. Available: https://articles.forensicfocus.com/2014/04/14/windows-forensics-and-security/. [Accessed: 12-May-2019].

[23] “What is network forensics? - Definition from WhatIs.com.” [Online]. Available: https://searchsecurity.techtarget.com/definition/network-forensics. [Accessed: 12-May-2019].

[24] “Determining the Best Acquisition Method | Information Assurance.” [Online]. Available: https://cyberdef.wordpress.com/2013/09/18/determining-the-best-acquisition-method/. [Accessed: 12-May-2019].

[25] “Windows Forensics Analysis Training | SANS FOR500.” [Online]. Available: https://www.sans.org/course/windows-forensic-analysis. [Accessed: 12-May-2019].

[26] “Registry Hives - Windows applications | Microsoft Docs.” [Online]. Available: https://docs.microsoft.com/en-us/windows/desktop/SysInfo/registry-hives. [Accessed: 12-May-2019].

[27] “Windows Registry Explained – Definitions, Purpose, Benefits | System Utilities Version 4.0 |The security products.” [Online]. Available: https://help.comodo.com/topic-159-1-290-3248-.html. [Accessed: 12-May-2019].

[28] “What is a Shortcut?” [Online]. Available: https://www.computerhope.com/jargon/s/shortcut.htm. [Accessed: 12-May-2019].

[29] “What is a Jump List?” [Online]. Available:

https://www.computerhope.com/jargon/j/jumplist.htm. [Accessed: 12-May-2019].

[30] "What is a Log?" [Online]. Available: https://www.computerhope.com/jargon/l/log.htm. [Accessed: 12-May-2019].

[31] "What is MFT (Master File Table)?" [Online]. Available: https://www.computerhope.com/jargon/m/mft.htm. [Accessed: 12-May-2019].

[32] "What is Dropbox." [Online]. Available: https://www.dropbox.com/features. [Accessed: 12-May-2019].

[33] "Dropbox Forensics | ForensicFocus.com." [Online]. Available: http://www.forensicfocus.com/dropbox-forensics. [Accessed: 12-May-2019].

[34] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, and K.-K. Raymond Choo, "Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices," *Aust. J. Forensic Sci.*, vol. 48, no. 6, pp. 615–642, 2016.

[35] "Mega (service)." [Online]. Available: https://en.wikipedia.org/wiki/Mega_(service). [Accessed: 12-May-2019].

[36] F. Daryabar, A. Dehghantanha, and K.-K. Raymond Choo, "Australian Journal of Forensic Sciences Cloud storage forensics: MEGA as a case study Cloud storage forensics: MEGA as a case study," 2016.

[37] "Microsoft OneDrive." [Online]. Available: https://onedrive.live.com/about/en-us/. [Accessed: 12-May-2019].

[38] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, and K.-K. R. Choo, "Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices," *Aust. J. Forensic Sci.*, vol. 48, no. 6, pp. 615–642, Nov. 2016.

[39] "What Is Amazon S3? - Amazon Simple Storage Service." [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html. [Accessed: 12-May-2019].

[40] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage

services," *Digit. Investig.*, vol. 9, no. 2, pp. 81–95, Nov. 2012.

[41] V. Roussev, A. Barreto, and I. Ahmed, "Forensic Acquisition of Cloud Drives *," 2016.

[42] D. Quick and K.-K. R. Choo, "Google Drive: Forensic analysis of data remnants," *J. Netw. Comput. Appl.*, vol. 40, pp. 179–193, Apr. 2014.

[43] M. S. Chang, "Forensic Analysis of Google Drive on Windows," 2016.

[44] T. Khairallah, "Cloud Drives Forensic Artifacts A Google Drive Case," Jan. 2019.

[45] S. T. Fabio Marturana, Gianluigi Me, "A case study on digital forensics in the cloud," *IEEE*, 2012.

[46] S. H. Mohtasebi *et al.*, "Tel: +44 (0)161 295 3531. A.Dehghantanha@Salford.ac.uk 3-Kim-Kwang Raymond Choo," Elsevier.

[47] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," 2012.

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

[49] "Wireshark · Go Deep." [Online]. Available: https://www.wireshark.org/. [Accessed: 12-May-2019].

[50] "FTK Imager 3.4.2." [Online]. Available: http://marketing.accessdata.com/ftkimager3.4.2. [Accessed: 12-May-2019].

[51] "Memory Forensics and Analysis Using Volatility." [Online]. Available: https://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/#gref. [Accessed: 12-May-2019].

[52] "Volatility 2.6 Release." [Online]. Available: https://www.volatilityfoundation.org/26. [Accessed: 12-May-2019].

[53] "Autopsy." [Online]. Available: https://www.sleuthkit.org/autopsy/. [Accessed: 12-May-2019].

[54] “Mft2Csv.” [Online]. Available: https://github.com/jschicht/Mft2Csv/wiki/Mft2Csv. [Accessed: 12-May-2019].

[55] “JumpListsView - View jump lists information stored by Windows 7.” [Online]. Available: https://www.nirsoft.net/utils/jump_lists_view.html. [Accessed: 12-May-2019].

[56] “Working with Registry View - Computer Forensics with FTK.” [Online]. Available: https://subscription.packtpub.com/book/hardware_and_creative/9781783559022/3. [Accessed: 12-May-2019].

[57] “An Introduction to the Windows System State Analyzer - Microsoft Tech Community - 374471.” [Online]. Available: https://techcommunity.microsoft.com/t5/Ask-The-Performance-Team/An-Introduction-to-the-Windows-System-State-Analyzer/ba-p/374471. [Accessed: 12-May-2019].

[58]! “ ! 2.4!Edition!” [Online]. Available: www.memoryanalysis.net!! [Accessed: 13-May-2019].

[59] “Whois.com - Domain Names & Identity for Everyone.” [Online]. Available: https://www.whois.com/. [Accessed: 12-May-2019].

[60] “DigitalOcean API.” [Online]. Available: https://developers.digitalocean.com/documentation/spaces/. [Accessed: 12-May-2019].

[61] “About regions.” [Online]. Available: https://support.rackspace.com/how-to/about-regions/. [Accessed: 12-May-2019].

[62] “Object services operations - Rackspace Developer Portal.” [Online]. Available: https://developer.rackspace.com/docs/cloud-files/v1/storage-api-reference/object-services-operations/#show-object-metadata. [Accessed: 12-May-2019].

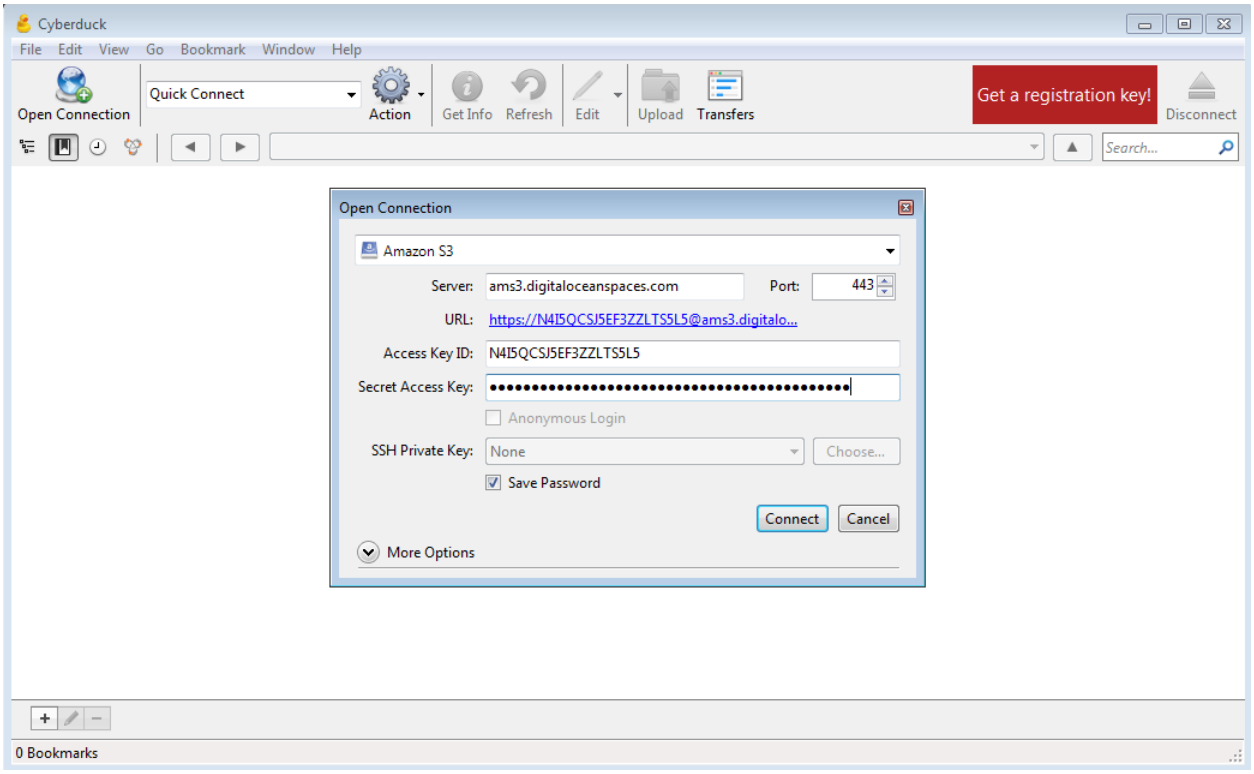
[63] H. R. Ahmadi, A. Mourad, R. Tawil, and M. B. Awada, “A New Approach in Digital Forensics Investigation Process,” in *2018 International Conference on Computer and Applications (ICCA)*, 2018, pp. 1–275.

[64] “iterate GmbH.” [Online]. Available: https://iterate.ch/. [Accessed: 12-May-2019].

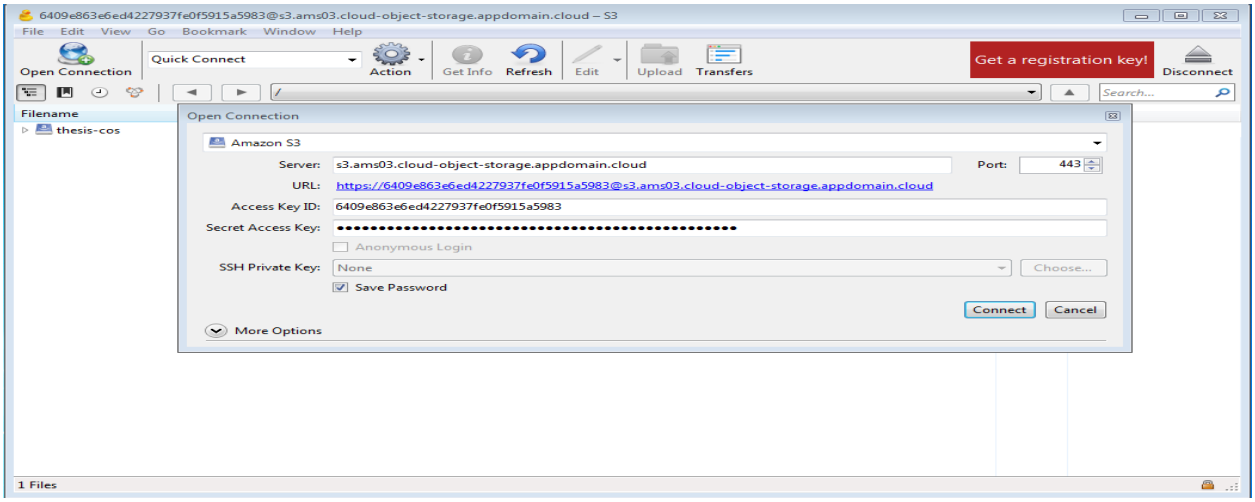
[65] “help/en/faq – Cyberduck.” [Online]. Available: https://trac.cyberduck.io/wiki/help/en/faq. [Accessed: 13-May-2019].

Appendix A

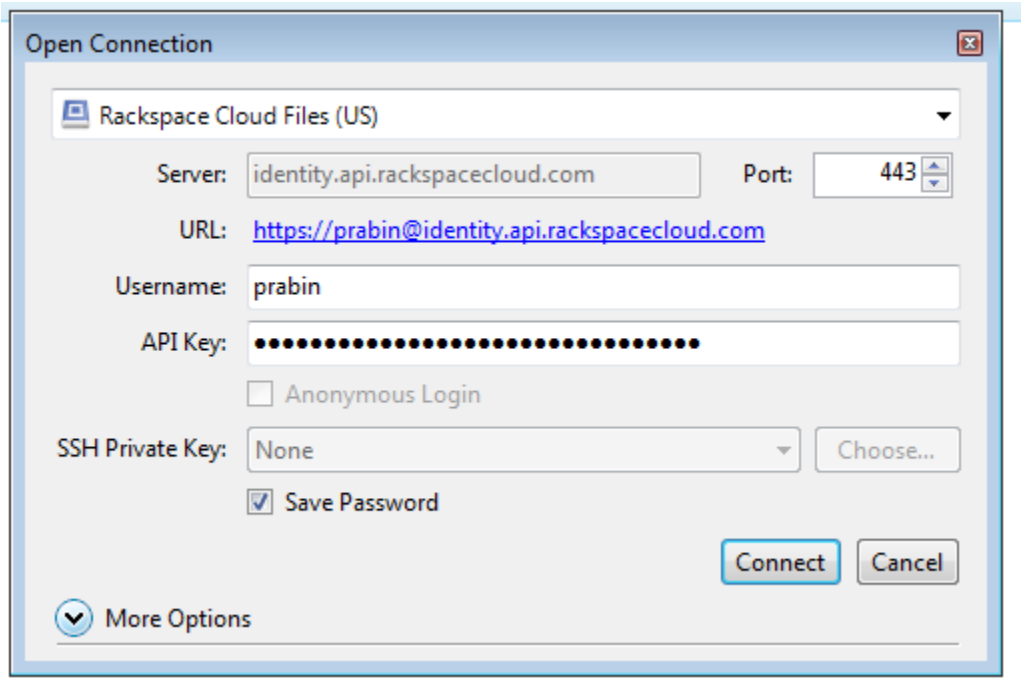
Cyberduck DO Spaces Connectivity Setup



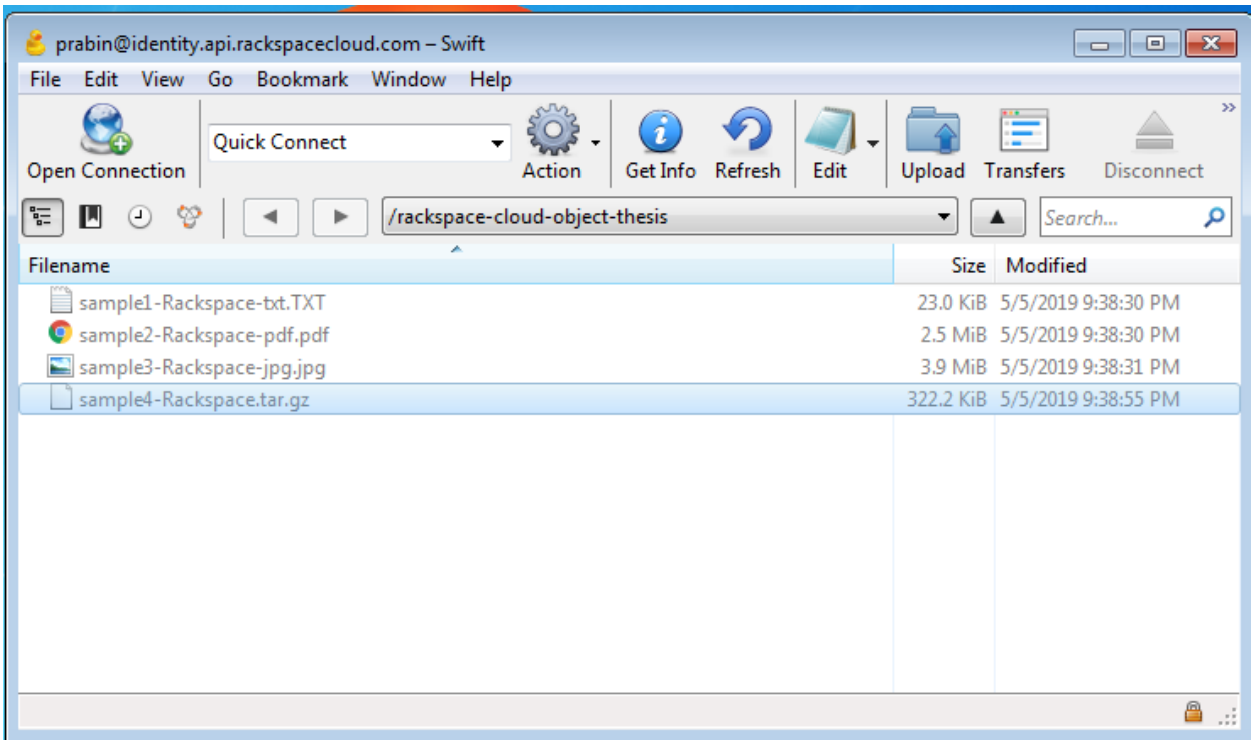
Cyberduck IBM COS Setup



Cyberduck Rackspace Cloud files setup

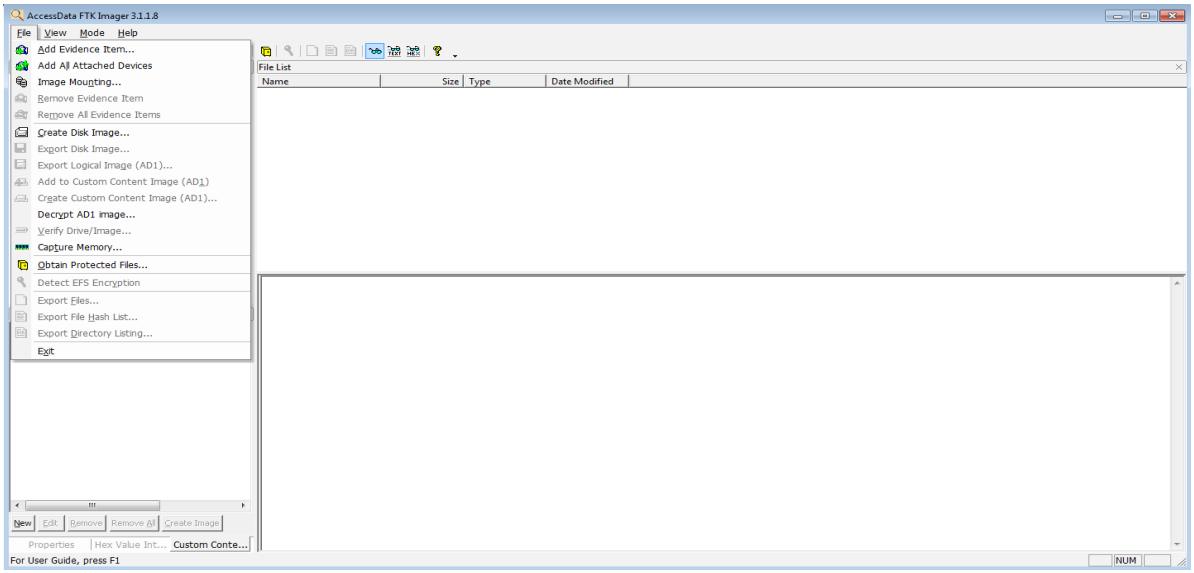


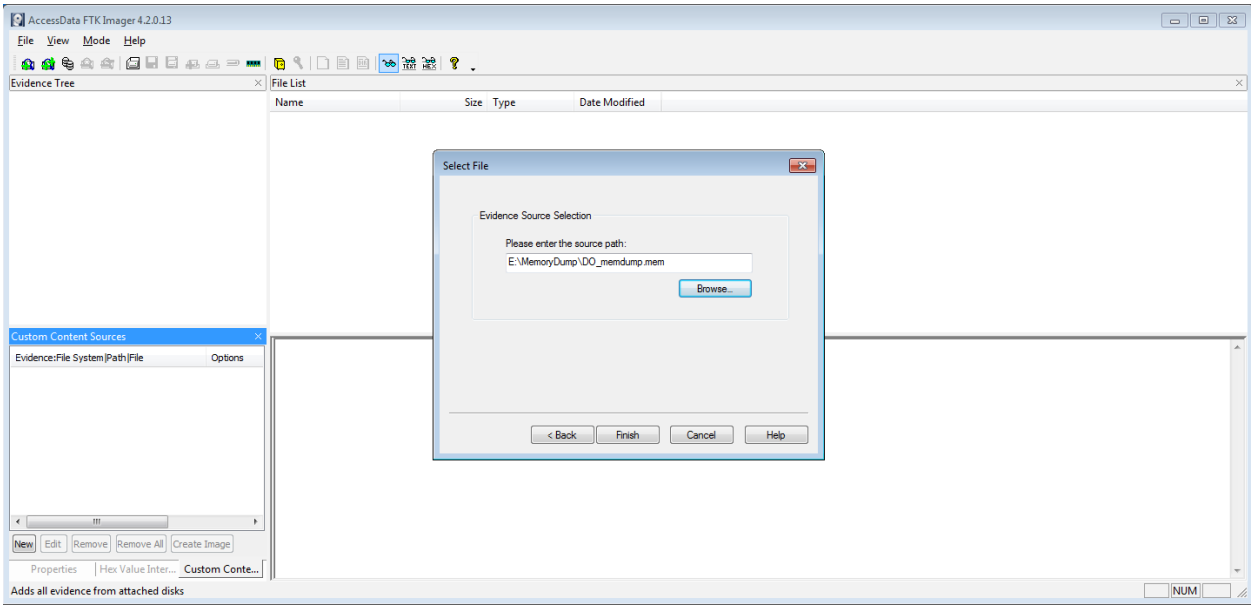
Cyberduck Disconnect

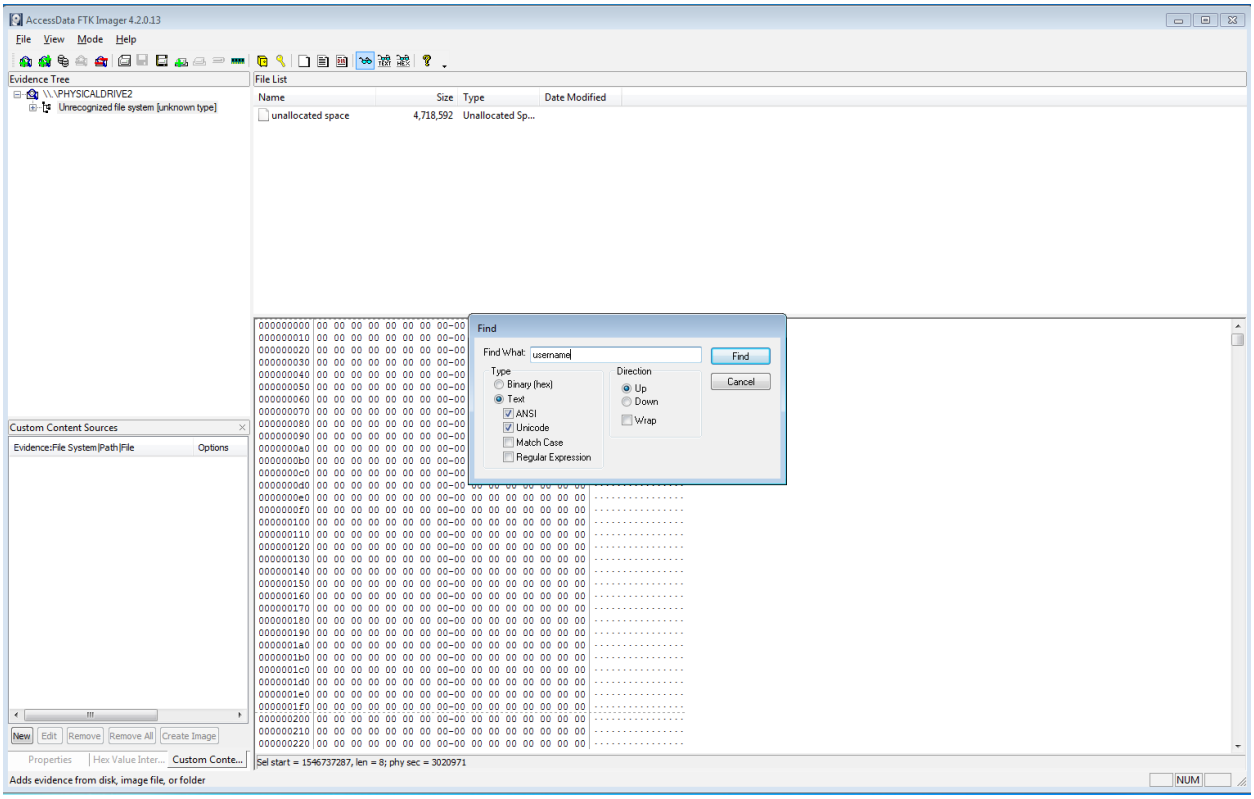


APPENDIX B

FTK Memory Acquisition







Local storage and Remote DO spaces Information's extracted from FTK imager

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

<key>Type</key>

<string>sync</string>

<key>Host</key>

<dict>

<key>Protocol</key>

<string>s3</string>

<key>Provider</key>

<string>iterate GmbH</string>

<key>UUID</key>

<string>82147646-08ac-4866-8387-c3e3a6340f1a</string>

<key>Hostname</key>

<string>ams3.digitaloceanspaces.com</string>

<key>Port</key>

<string>443</string>

<key>Username</key>

<string>N4I5QCSJ5EF3ZZLTS5L5</string>

<key>Workdir Dictionary</key>

<dict>

<key>Type</key>

<string>[directory, volume]</string>

<key>Remote</key>

<string>/thesis-space</string>

<key>Attributes</key>

<dict>

</dict>

</dict>

```
        <key>Upload Folder Dictionary</key>
        <dict>
                <key>Path</key>
                <string>C:\Users\prabin\Desktop</string>
        </dict>
        <key>Access Timestamp</key>
        <string>1556744143439</string>
</dict>
<key>Items</key>
<array>
        <dict>
                <key>Remote</key>
                <dict>
                        <key>Type</key>
                        <string>[directory, volume]</string>
                        <key>Remote</key>
                        <string>/thesis-space</string>
                        <key>Attributes</key>
                        <dict>
                        </dict>
                </dict>
                <key>Local Dictionary</key>
```

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis_files</string>

</dict>

</dict>

</array>

<key>UUID</key>

<string>49c5db82-9922-40df-8bf8-9eef8745d190</string>

<key>Size</key>

<string>0</string>

<key>Current</key>

<string>0</string>

<key>Bandwidth</key>

<string>-1.0</string>

<key>Action</key>

<string>ask</string>

</dict>

Cyberduck Transfer file xml file sample

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>Type</key>
	<string>sync</string>
	<key>Host</key>
	<dict>
		<key>Protocol</key>
		<string>s3</string>
		<key>Provider</key>
		<string>iterate GmbH</string>
		<key>UUID</key>
		<string>6f0a78e6-4d61-4a2d-95eb-0ef18a5498d3</string>
		<key>Hostname</key>
		<string>ams3.digitaloceanspaces.com</string>
		<key>Port</key>
		<string>443</string>
		<key>Username</key>
```

<string>N4I5QCSJ5EF3ZZLTS5L5</string>

<key>Upload Folder Dictionary</key>

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop</string>

</dict>

<key>Access Timestamp</key>

<string>1555785258841</string>

</dict>

<key>Items</key>

<array>

<dict>

<key>Remote</key>

<dict>

<key>Type</key>

<string>[directory, volume]</string>

<key>Remote</key>

<string>/thesis-space</string>

<key>Attributes</key>

<dict>

</dict>

</dict>

```
                <key>Local Dictionary</key>
                <dict>
                        <key>Path</key>
                        <string>C:\Users\prabin\Desktop\thesis_files</string>
                </dict>
        </dict>
</array>
<key>UUID</key>
<string>aeab9c95-e325-4c15-b493-8452d1bf5ae0</string>
<key>Size</key>
<string>0</string>
<key>Current</key>
<string>0</string>
<key>Timestamp</key>
<string>1555786268204</string>
<key>Bandwidth</key>
<string>-1.0</string>
<key>Action</key>
<string>mirror</string>
</dict>
</plist>
```

APPENDIX C

Rackspace Cloud Files

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Type</key>
    <string>upload</string>
    <key>Host</key>
    <dict>
        <key>Protocol</key>
        <string>swift</string>
        <key>Provider</key>
        <string>iterate GmbH</string>
        <key>UUID</key>
        <string>e81abaf2-addc-440a-acc8-5b34466fd25a</string>
        <key>Hostname</key>
        <string>identity.api.rackspacecloud.com</string>
        <key>Port</key>
        <string>443</string>
        <key>Username</key>
        <string>prabin</string>
```

<key>Access Timestamp</key>

<string>1557070354909</string>

</dict>

<key>Items</key>

<array>

<dict>

<key>Remote</key>

<dict>

<key>Type</key>

<string>[file]</string>

<key>Remote</key>

<string>/rackspace-cloud-object-thesis/sample1-Rackspace-txt.TXT</string>

<key>Attributes</key>

<dict>

<key>Region</key>

<string>IAD</string>

</dict>

</dict>

<key>Local Dictionary</key>

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis-rackspace\sample1-Rackspace-txt.TXT</string>

</dict>

</dict>

<dict>

<key>Remote</key>

<dict>

<key>Type</key>

<string>[file]</string>

<key>Remote</key>

<string>/rackspace-cloud-object-thesis/sample2-Rackspace-pdf.pdf</string>

<key>Attributes</key>

<dict>

<key>Region</key>

<string>IAD</string>

</dict>

</dict>

<key>Local Dictionary</key>

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis-rackspace\sample2-Rackspace-pdf.pdf</string>

</dict>

</dict>

<dict>

<key>Remote</key>

<dict>

<key>Type</key>

<string>[file]</string>

<key>Remote</key>

<string>/rackspace-cloud-object-thesis/sample3-Rackspace-jpg.jpg</string>

<key>Attributes</key>

<dict>

<key>Region</key>

<string>IAD</string>

</dict>

</dict>

<key>Local Dictionary</key>

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis-rackspace\sample3-Rackspace-jpg.jpg</string>

</dict>

</dict>

<dict>

<key>Remote</key>

<dict>

<key>Type</key>

<string>[file]</string>

<key>Remote</key>

<string>/rackspace-cloud-object-thesis/sample4-Rackspace.tar.gz</string>

<key>Attributes</key>

<dict>

<key>Region</key>

<string>IAD</string>

</dict>

</dict>

<key>Local Dictionary</key>

<dict>

<key>Path</key>

<string>C:\Users\prabin\Desktop\thesis-rackspace\sample4-Rackspace.tar.gz</string>

</dict>

</dict>

</array>

<key>UUID</key>

<string>5a4d64ce-e81c-430d-bdb4-fa5ac9956cf3</string>

<key>Size</key>

<string>7046000</string>

<key>Current</key>

<string>7046000</string>

<key>Timestamp</key>

<string>1557070390409</string>

<key>Bandwidth</key>

<string>-1.0</string>

</dict>

</plist>

APPENDIX D

MD5sum of acquired disk Image during disk acquisition on our analysis.

Disk Name	Md5sum	Associated Cloud Storage	Disk Analysis
DO_Cyberduck_Case1.E01	f1d9f79678eee51b43dd90878dc7d892	DO Space	1
IBM_COS_Case 2 .E01	5e5a24c1d14379576823bc00e571845e	IBM COS	1
\Rackspace_Cyberduck_case 3.E01	c8b3ad676a9d1f77ef20d30a74c96b4f	Rackspace	1
DO_Space_Image_file_deleted_1.1.E01	6e1d875658ff207f02d92879f5de27e9	DO Space	2
IBM_DISK_Analysis_DeletedFile2.1.E01	281eb608f1c0f540e9ccd130304d0d36	IBM COS	2
Rackspace_delete_file_analysis_3.1.E01	5aa31f29e5e6d2f97a5fa5eae7c4d2be	Rackspace	2