Cloud Digital Forensics Evaluation and Crimes Detection

Raja Jabir(✉) and Omar Alfandi

College of Technological Innovations, Zayed University, Abu Dhabi, UAE
{M80006379,Omar.Alfandi}@zu.ac.ae

Abstract. Cloud computing is one of the significant topics of today's era; due to the enhancement it brings to the Information Technology world. This transformation lead to its rapid adoption by different sectors, ranging from enterprise to personal usage. Organizations are constantly looking for ways to increase productivity with optimum cost; which derived the need for Cloud environments and its underlying virtualized infrastructure. With the increase usage of Cloud based infrastructure, criminals utilized its anonymity factor to hide their criminal activities; escaping from legal actions. This paper highlights the obstacles experienced during Cloud virtual layer forensics acquisition and analysis, due to lack of specialized forensics tools. We have developed a framework to aid in assessing the virtual environment readiness for forensics investigation and examine the applicability of existing state-of-the-art forensics tools to Cloud environment. The paper reveals the need for having specialized forensics tools for Cloud infrastructure forensics.

Keywords: Cloud computing · Virtual layer · Digital forensics · Cloud forensics · Forensics analysis · Dropbox

1 Introduction

Cloud computing has significantly transformed the way Information Technology (IT) services are being perceived. This advancement of technology has changed the traditional (IT) resource utilization and consumption, enabling IT service providers to meet organizations needs for high-end solutions with optimum cost. Cloud is built on the concept of resource sharing, where a pool of resources are accessed over the network on demand [1]. Cloud characteristics, as defined by National Institute of Standards and Technology (NIST), are an on demand self service, resource pooling, wide network access, and rapid elasticity [1]. The fundamental part of Cloud computing is the virtual layer; that serves as a platform to optimize resource utilization, transforming a single physical server into multiple virtual servers, thus increasing return on investment by reducing the overhead costs.

This growth in Cloud usage has raised concerns about security, integrity and privacy of data residing in a Cloud environment. With the diverse usage of Cloud environment and its unique nature, it enables additional functionalities such as IT computational outsourcing and sharing of resources, the concern of using Cloud as a platform for cybercrimes is increasing. From a security standpoint, it is critical for law enforcement

F. Belqasmi et al. (Eds.): AFRICATEK 2017, LNICST 206, pp. 171–180, 2018.
https://doi.org/10.1007/978-3-319-67837-5_16

and digital forensics investigators to detect and solve criminal cases conducted using Cloud platforms. Unfortunately, the field of Cloud forensics is still immature with limited support from specialized digital forensics tools. This is possibly due to unavailability of standardization and interoperability between different Cloud vendors and deployed infrastructures.

This paper proposes a framework to examine the current state of Cloud virtual layer forensics. Experiments are conducted using three VMware ESXi Servers; due to its wide deployment across various enterprises. Servers hard disk images are acquired and examined using different forensics analysis tools. Anti-forensics activities, such as detecting deleted artifacts, is performed. Cloud Storage applications (exemplified using Dropbox) analysis is conducted to analyze traces availability. As a result of this research, we were able to highlight the tools that are applicable for Cloud forensics analysis.

2 Background

During the experiments we used a cluster of three Servers with VMware ESXi installation, a popular proprietary enterprise hypervisor provided by VMware. ESXi is installed on the physical servers to create a virtualization layer between the server and the operating systems [2]. This proprietary hypervisor utilizes the physical server 'host' resources such as memory, processor, network and storage, and virtually present them to several instances of virtual machines 'guest' [2]. The created virtual machines (VM) can run different operating systems independently of the host operating system and independently of each other; as each VM has its own operating system, memory, BIOS, network and storage. The hypervisor is responsible for this segregation between 'guests' and 'host' by the implementation of virtualization layer. VMware ESXi was chosen as the experiment environment due to its wide deployment and increasing market margin.

3 Literature Review

Cloud computing is rapidly being implemented in different domains from enterprise to personal usage. Due to its capability and cost efficiency organizations are moving toward Cloud infrastructure, aiming to reduce their operation expenses. Despite Cloud wide implementation across the world and the increase usage of Cloud in criminal activities, there is limited research on the area of Cloud forensics, leading to lack of awareness about Cloud issues [3]. Ali et al. [4] explained the different available Cloud models today; stressing on the associated security threats targeting the different Cloud components. Some of the threats discussed are virtual network vulnerabilities, threats on the communication layer, and privacy concerns due to user inadequate control on their data. The Authors discussed important security measures such as applying identity management and access control technologies. Pichan et al. [5] also provided a broad explanation of Cloud challenges and the different solutions; highlighting Cloud issues such as unknown geographical location, jurisdiction, encryption, and decentralized data. The Authors used the traditional digital forensics framework as a platform for assessing and analyzing the current Cloud issues.

From the security perspective, understanding the security threats and exploits in a Cloud environment is imperative to take proactive protective actions. Khorshed et al. [6] identified that the main Cloud challenges are trust issues, security risks and security threats. Other Cloud challenges [7] included application security, information leakage, data segregation, and privacy due to exploits of data confidentiality. To address these issues the Authors proposed applying fine grained access control and RSA encryption mechanism to avoid data disclosure; however this increases the complication of the Cloud forensics investigation process.

One of the main obstacles facing digital forensics examiners is data acquisition, that is critical to be conducted efficiently [8]. Preservation of possible evidentiary data during the acquisition and collection process is crucial; to ensure its integrity and admissibility in the court of laws. Quick and Choo [9] addressed the data integrity challenges during the evidence collection process, by utilizing public cloud storage providers such as Google Drive and Dropbox. The Authors findings presented that files metadata remains unchanged during the process of uploading, storing and downloading. This is applicable for unaltered files, which is difficult to control in a Cloud environment where files are shared and modified by different individuals. The Authors also illustrated changes in downloaded files timestamps when compared to the original file, which may hinder the forensics investigation process.

With Cloud forensics being a relatively immature domain it is important for a forensics examiner to understand the nature of artifacts stored in a Cloud environment; to support the forensic examination and analysis process. Martini and Choo [10] examined the artifacts available in Storage-as-a-Service Cloud model 'ownCloud' on both the client and server sides, categorized them and assessed their relevance to the forensics investigation process. The Authors assessed the stored files metadata and the authentication artifacts, highlighting their importance in identifying the Cloud instance used in any criminal activities and linking those acts to Cloud users.

This research will discuss the current state of Cloud environment, customizing traditional digital forensics framework and tools to meet Cloud unique requirements. Moreover this research will also determine detection of anti-forensics activities such as intentionally deleting artifacts. The research will exemplify Cloud readiness for forensics investigations and the experienced challenges.

4 Experimental Setup

The purpose of the experiments was to imitate real life scenarios and study the type of artifacts most likely to be involved in a Cloud environment crime scene. The presented framework is applicable to forensically analyze various Cloud environments. It consists of the following main sections:

(1) *System Preliminary Assessment*: Host examination for any virtual instances traces and artifacts was conducted by performing manual search and analysis; in order to collect any available artifacts and identify their location in the Cloud virtual layer.
(2) *Host Forensics Analysis*: Acquisition and forensics analysis of the selected ESXi Servers was conducted using commercial and open source digital forensics tools.

This is to determine the applicability of the current digital forensics process and tools to Cloud virtual environment.

(3) *Cloud Storage Forensic Analysis*: Forensics examination and analysis for the artifacts created on a Host during the installation and usage of a Cloud Storage Application was performed. This aims to identify and study the type of evidence created when such storage applications are used, and to assess the level of security implemented by these applications.

A. ESXi Servers

During the experiments we used a cluster of three Servers with VMware ESXi installation, a popular enterprise hypervisor provided by VMware. Each server had five physical internal SATA hard drives, each with a storage capacity of 500 GB. The servers were managed using vCenter server which was used to create new virtual machines and allocate storage space. In addition the system was connected to a VNX storage system, in which created virtual machines configurations and data files were stored.

B. Performed activities

The experiment was designed to simulate real life scenarios that will be utilized for subsequent investigations. Virtual Machines were created and assigned to users to perform certain activities such as log-in/log-off from the assigned machines, accessing the internet, creating and deleting files; which is important to investigate anti-forensics actions. In addition Dropbox Cloud Storage application was installed and used to upload and delete files from the Cloud storage service application. The objective is to investigate the artifacts that are created when users perform these activities.

C. Forensics Acquisition

To acquire the ESXi Servers hard disk images, each hard drive was removed and using an ATA serial cable we connected the hard disk to a Tableau SATA bridge, which also functions as a write-blocker. This is critical to avoid contaminating and tampering the original servers hard drive while performing the image acquisition. FTK Imager software was used to physically acquire the images, in raw format, and validate them by generating two checksums MD5 and SHA1; to ensure their integrity and detect any errors. The image acquisition process was a lengthy process that consumed approximately eight hours for each Hard Disk.

D. Forensics Analysis

We used the best available digital forensics tools throughout our experiments. The selection was based on the popularity and relevance. The tools used are as follows:

(1) *X-Ways forensics*: The tool did not allow exploring the disk images file systems. However it was able to display the disk images in chunks (318 chunks), which means the investigator should manually open each chunk separately and perform the analysis. It was also used to perform keyword search for server name, usernames and used applications. We were able to locate the server name, type and public key token. This is a tedious process if the search keywords are not known in advance; being the case in a criminal case investigation.

(2) *Autopsy*: We used Autopsy 4.0 to perform keyword search. It was more effective then X-Ways, as it displayed the entire image in a single window rather than dividing it into 318 chunks and having to analyze each chunk individually. The tool detected the system partition, as it supports internal file system structure. Utilizing the keyword search feature in Autopsy, it displayed details about the volume. The details are: full volume name, type as 'File system', it being an allocated space, date of creation, modification and access, Internal system ID, and finally the volume MD5 hash value. Furthermore the search also displayed information about the VMware ESXi boot details and configuration file. In addition Autopsy also displayed details about a deleted file, which was placed in the disk unallocated space. This file contained information about a deleted virtual machine configuration and the guest operating system as 'windows 7-64', the vCenter unique ID, ethernet card address, guest and host CPU ID. Theses information can be useful during the investigation process.

(3) *Magnet Internet Evidence Finder (IEF)*: version 6.7 was used as it is known to support artifacts analysis from different computer domains such as gaming consoles and Cloud storage applications. The image parsing consumed about three hours, after which the results were displayed. The software provided information about the file system type, number of available sectors, volume name and number, and source details. In addition information about system identifiers were retrieved. The Security User ID was displayed for accounts that accessed the ESXi Server, with a corresponding 'Artifact ID'. We then used this ID to map it with an entry in the Windows Event Logs; in order to associate an action with a specific user security ID. The information retrieved are the Event ID, the associated Security User ID, date and time the event occurred, and finally events description. Another interesting detected information is details about users login and log-off actions on the ESXi server. This is important for audit trailing, and associating an activity to a particular user.

(4) *ProDiscover*: Version 7 was used as it includes options to view registry entries and to retrieve deleted files and images. Details retrieved are image type 'DD image', total sectors size, total image size, the volume name 'ESXi', volume serial number (only ProDiscover and IEF Magnet detected this information), File System type, total clusters and sectors per cluster, the image starting and ending sectors. However, unlike Autopsy it did not detect the deleted system files.

E. Cloud Storage Application Forensic

These applications popularity is increasing, with shifts from the standard home users to businesses who are utilizes them for file sharing, document backups and other various activities. Cloud storage service providers are competing to supply additional features and even developing mobile applications to allow users to access their files, that were uploaded to the service website, on the go without geographical restrictions. These services allowed automatic data synchronization for any modification performed using any of the installed application connected to the cloud storage account. For example, when you upload a new document from your laptop, this file will be available when logging from your mobile device.

For this experiment, we studied the Cloud storage forensics implications, Dropbox was used to exemplify Cloud Storage applications; in order to examine the nature of artifacts produced once the application is installed and used. Initially signed-up for the Dropbox service and then downloaded the application on a virtual machine. The application created a directory under the used user's profile, and contained all user's Dropbox documents, which is considered as an offline cache of the Dropbox account documents. This is important to synch accounts data, and so it was reflected in the user's local 'Dropbox' folder.

5 Experimental Results

5.1 System Manual Examination

This phase addresses the major challenge of audit trailing in a virtual environment. In this aspect, artifacts that can be linked to virtual machine users were investigated. We found that when a virtual machine is launched, several files were created in the host machine under the virtual machine home directory. These files are used to allow the communication between the host and guest operating system. Artifacts that can associate actions to users of a virtual machine instance 'guest VM' were searched. In the investigation we focused on identifying artifacts about the virtual machine instance users, installed/used applications, and other metadata such as date and time of mentioned actions.

In this experiment, we used VMware, which created a directory called 'caches' in the host machine under the virtual machine home directory. Inside 'caches' folder, another directory was created called 'GuestAppsCache' which included two main subdirectories 'appData' and 'launchMenu'. On browsing the 'appData' folder contents, several files were found each named with a 32 character hex format. Each name was repeated twice with two different file types 'APPICON' and 'APPINFO'. The file information such as modification date, time, and size were available. For example, a files called '0e469eee0c8567ed0659732027f7ce54.appicon' of size 52 KB and a its corresponding file called '0e469eee0c8567ed0659732027f7ce54.appinfo' were created on the same time, with the preceding being of 1 KB size. We then extracted the files and viewed them using a Hex editor. The '0e469eee0c8567ed0659732027f7ce54.appicon' file contained information about VM users and launched applications and the corresponding file '0e469eee0c8567ed0659732027f7ce54.appinfo' contained information about the appicon file in a human readable format. As part of our observation, it was noticed both 'APPINFO' and 'APPICON' file types were created when the virtual machine users launch any application.

The second folder was called 'launchMenu', and contained a file called 'launchMenu.menudata'. This file had information about the virtual machine Start Menu shortcuts. By associating the date and time of the file, an audit trail was established. This is important for activity monitoring and audit trailing, as it helps in associating an action on a virtual machine to the right user. Using these information we were able to establish a chain of events; aiding in crime detection.

In addition deleted artifacts were examined in attempt to determine anti-forensics activities. An experiment included deleting an application from a virtual machine and checking if the corresponding files '.APPICON' and '.APPINFO' on the host were deleted or not. Interestingly, these files existed and were not removed. This is important during a crime scene investigation in which criminals attempt to delete their traces as a form of anti-forensics activity.

5.2 Image Forensics Analysis

VMware ESXi Server 'Host' forensics analysis and examination was conducted utilizing the most reliable traditional digital forensics software in the market. It is imperative for a forensics investigator to be able to validate the forensics software outcome; to ensure results reliability and integrity. This was achieved by utilizing different tools and performing a comparison of their outcome, detecting any inconsistency and error rates. These tools also save effort by automating the process of searching for artifacts of evidentiary nature located across the forensic image. We used four different forensics software X-Ways Forensics, Autopsy, Magnet Internet Evidence Finder and ProDiscover. These tools were used to conduct a thorough and exhaustive analysis on the forensically acquired image of the ESXi Server using FTK Imager and a write blocker; to prevent original evidence contamination.

Most of the tools detected the ESXi partitions but failed to parse them and retrieve evidentiary information. Magnet IEF was the best out of the investigated tools. However it failed to retrieve deleted files like Autopsy. Each tool retrieved different information making it difficult to validate their accuracy and error rate. This indeed proved the incompatibility of current available digital forensic tools to parse and analyze Cloud virtual layer image. This requires vendors to develop specialized digital forensics tools customized to meet the Cloud environment needs (Table 1).

Table 1. Artifacts summary

Forensics tool	Retrieved artifacts
X-Ways forensics	Keyword search: server name, server type, public key token
Autopsy 4.0	Keyword search: server name, server type, volume name and type of space (allocated), date of creation/modification/access, Internal system ID Deleted files: Information about guest OS, vCenter ID, guest & host CPU ID
Magnet IEF 6.7	File system type, number of available sectors, volume details, security user ID, events details (such as login/logoff actions)
ProDiscover 7	Total sectors/image size, volume name, volume serial number, File System type, total clusters and sectors per cluster, the image starting and ending sectors

5.3 Cloud Storage Application Forensics

Several files were retrieved from the Dropbox directory, and have been investigated to detect useful artifacts. The investigated files and directories are [12]:

- **config.dbx**: This is an SQLite file that included information about the associated Dropbox account, email address, and installation related information.
- **filecache.dbx**: This file is consisted of tables. It includes information about the files inside the users' Dropbox directory.
- **bin**: This folder includes the executable files that are used by Dropbox application.

Further analysis was performed using Magnet IEF tool that allowed the decryption of both config.dbx and filecache.dbx file.

- Config.dbx file displayed the Dropbox associated email address 'xxx@gmail.com'.
- filecache.dbx file displayed records of all the available folders, files and images in the Dropbox account under investigation. The information obtained are file name, file path, creation date and time, modification date and time, file size, file version ID; this is used by Dropbox to avoid data duplication optimizing storage space utilization. All entries were located in the 'file_journal' table.

5.4 Countermeasures

As a security measure, we applied encryption to all confidential files before uploading them to the Cloud storage application. Boxcryptor application was installed on the our virtual machine. This software created a drive that is connected to the user's Cloud Storage application. By saving the files in this drive we can encrypt and decrypt them instantly. All files saved to the drive were found to be reflected in the Dropbox folder; which were then synchronized to the Dropbox account.

6 Analysis and Discussion

The conducted experiments' outcome demonstrated the limitation of the specialized state-of-the-art digital forensics analysis tools. This is clearly due to Cloud being a relatively new domain, with limited research and knowledge. The retrieved artifacts were a result of our preceding knowledge such as system type and sequence of conducted events, which is not applicable to traditional crime investigations.

From the vendor perspective, they are competing to deploy enhanced high level security mechanisms in an attempt to combat criminal attempts to invade Cloud users confidentiality and privacy. This study aims at directing the focus of forensics investigation to Cloud environment, due to its increasing large deployment scale, and its future of being a rich source of digital evidences.

7 Challenges and Limitations

Despite the advantages introduced with the implementation of Cloud setup, there are drawbacks to this technology, that affects the digital forensics investigation process:

- Limited documentation about Cloud setup and virtualization layer specifically.
- Inadequate knowledge and lack of trained and expert digital forensics investigators in Cloud environment.
- Vendors implementation of proprietary file systems and hypervisors, which is an unsupported format by most of the existing digital forensics tools.
- Lack of specialized Cloud forensics tools that are specialized in virtual systems and distributed systems.
- Limited control on the data stored in Cloud environment.
- Multiply users, so it is difficult to identify system users and data owners.
- It is difficult to retrieve evidences that are stored in Cloud, as its might involve breaching the confidentiality of other Cloud users.
- Hard to produce a forensically sound evidence to be accepted in court.
- Legal restrictions, as systems hosting Cloud infrastructure reside on different geographical locations (can be different countries) each with its own laws and regulations.
- Service providers are not cooperative, with each Cloud provider having different Cloud computing setup and approaches.

8 Recommendations

Enhancing the process of Cloud forensics, involves cooperation between all stakeholders to contribute to Cloud and its underlying components readiness for digital forensics investigations. Below are some of the recommendations:

- Introducing legal regulations, that enforces cooperation between all countries hosting cloud infrastructure.
- Training digital forensics investigators and examiners, to be Cloud experts.
- Educating users on the risks of Cloud systems, such as data privacy and confidentiality.
- Cooperation of Cloud service providers with digital investigations, providing information about the implemented systems and proprietary hypervisors.
- Developing specialized tools, policies, and procedures for Cloud forensics, that is customized to meet Cloud requirements.

9 Conclusion

In this paper, we assessed the current state of Cloud computing forensics, to evaluate its readiness for digital forensics analysis and investigation. The most reliable digital forensics applications were utilized to test their applicability to Cloud environment needs. During the experiment, all four used tools detected the ESXi Server system partition.

Manual host examination provided useful information that can be used for audit trailing, which is one of the major Cloud issues today. This research directs the spotlight to the need of specialized Cloud tools that are virtualization compatible, and it also aims at increasing awareness about the significance of establishing partnerships with Cloud Service Providers for forensics investigators to be up to date with the advancement of technology and establish understanding about the type of Cloud artifacts.

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing (2011)
2. VMware, E.S.X., ESXi, V.: The market leading production-proven hypervisors. vmware. Disponível em: http://www.vmware.com/files/pdf/VMware-ESX-and-VMware-ESXi-DS-EN.pdf. Data de Acesso 11(11) (2009)
3. Harichandran, V.S., Breitinger, F., Baggili, I., Marrington, A.: A cyber forensics needs analysis survey: revisiting the domain's needs a decade later. Comput. Secur. **57**, 1–13 (2015)
4. Ali, M., Khan, S.U., Vasilakos, A.V.: Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015)
5. Pichan, A., Lazarescu, M., Soh, S.T.: Cloud forensics: technical challenges, solutions and comparative analysis. Digit. Invest. **13**, 38–57 (2015)
6. Khorshed, M., Ali, A., Wasimi, S.: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Futur. Gener. Comput. Syst. **28**(6), 833–851 (2012)
7. Rao, R., Velumadhava, K.: selvamani: data security challenges and its solutions in cloud computing. Proced. Comput. Sci. **48**, 204–209 (2015)
8. Rozanski, S.: Using cloud data to accelerate forensic investigations. Netw. Secur. **2015**(9), 19–20 (2015)
9. Quick, D., Choo, K.K.R.: Forensic collection of cloud storage data: does the act of collection result in changes to the data or its metadata? Digit. Invest. **10**(3), 266–277 (2013)
10. Martini, B., Choo, K.K.: Cloud storage forensics: owncloud as a case study. Digit. Invest. **10**(4), 287–299 (2013)
11. Kent, K., Chevalier, S., Grance, T., Dang, H:. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication, pp. 800–886 (2006)
12. vmware. https://www.vmware.com/support/ws55/doc/