Chapter 7: New Digital Forensic Model to Support Cloud Computing in Investigation of Cybercrimes

Currently, Cloud Computing adopted by various societies, organizations, and governments so that it is becoming very urgent for providing cloud services with ensuring that Cloud Service Providers (CSPs) support the digital investigation process in a forensically sound and timely fashion manner. Cost effective of forensics design and implementation as part of cloud infrastructure to build cloud architecture support forensics is an important issue have to take into consideration to facilitate cloud forensics. Cloud Forensics has become an attractive research direction in cloud security domain. Performing the cloud forensics process pose voluminous intricate legal, organizational and technical challenges due to virtualization, distributing and dynamic nature of cloud systems. These challenges such as crime scene reconstruction, isolating cloud instance, data provenance, evidence segregation, need to be resolved to perform a convenient cloud forensics.

This chapter introduces the design and implementation of a new Cloud Forensics Investigation Model (CFIM) to investigate cybercrimes in the cloud environment. The proposed system is a smart system that is able to take a snapshot of the state of running virtual machine in virtual datacenter and send to Trusted Center Server (TCS) that monitor the status of the Virtual Machines (VMs) as well as store snapshots of the virtual machines for sending them for Forensic Server (FS) up to require for performing forensics process. The proposed model supports a concept of Forensics as a Service (Faas) that provide various benefits of conducting digital forensics through using Forensic Server on the cloud side. From experimental results, the proposed model can assist digital investigators to find and extract digital evidence as an admissible proof related to crime in a cloud environment. This can help to build new cloud infrastructures that support digital forensics especially critical sectors such as financial and healthcare which needs a special type of security due to its have critical and sensitive information.
The rest of this chapter is structured as follows: section 7.1 provides chapter introduction while related work is presented in section 7.2. Section 7.3 introduces the proposed Cloud Forensics Investigation Model (CFIM) while the implementation of the proposed model is presented in section 7.4. Finally, the chapter summary of this innovative research is presented in section 7.5.

### 7.1 Introduction

In the recent times, Cloud computing has become one of the most popular computing paradigms which adopted by several companies and organizations because it provides and offers numerous services that have a lot of benefits and advantages such as optimize the general usage of IT infrastructures, a high degree of scalability and availability of massive computing and storage resources. Cloud computing poses inimitable mixture of characteristics involving rapid elasticity, broad network access, measured service, and on-demand self-service. Cloud Computing consists of three main components which are Chain of Users, Chain of CSP, Chain of Services. Figure 7.1 shows the relation between User (U), Service (S) and CSP(C) in cloud environment which will help to understand the roles of them.

![Figure 7.1: Relation between User, Service and CSP in Cloud Environment.](image)

With the appearance of cloud computing technology that depends on a theory of distributing and dynamic nature of datacenters around the world to provide these services with a method of cost-per-use as well as the colossal amount of resources with cheap cloud computing services such as data storage. This makes the cloud systems subject to severe types of attacks by hackers and criminals, who may be able to hack and use these resources for illegal purposes, and also potentially can utilize the cloud to host or store evidence of their criminal data like terrorism-related materials. In addition to this, cloud services can also be used as a launching platform for new advanced types of attacks. Therefore, security
of cloud infrastructure represents a vigorous role for a guarantee to provide services for customers especially from ticklish community sectors including healthcare and finance that tardily accept the migration of their work to the cloud.

Performing cloud forensics process pose voluminous intricate jurisdictional, organizational and technical challenges identification and seize digital evidence from cloud systems by law enforcement and national security agencies, this due to virtualization, distributing and dynamic nature of cloud systems. These challenges and issues such as crime scene reconstruction, isolating cloud instance, data provenance and evidence segregation, can obstruct digital forensic investigators, law enforcement, and national security agencies and possibly prevent from acquiring and analyzing digital evidence in forensically and timely fashion manner. Also, this digital evidence may also be spread across several datacenters in diverse countries over the world, so that to collect, identify, and preserve data, there may legal and jurisdictional issues which needed to complete the forensics process to reconstruct crime events. This lead researchers and scientists to think for a solution that needs to be resolved to perform a convenient cloud forensics.

Currently, in cloud security area, some researchers focused on study data security in the cloud, and others are interested in digital forensics for exploring and identifying challenges and problems related to perform the digital investigation process in cloud environments as well as discuss an incident response strategies. A little number of them start to propose new tools, methods, techniques, and models to carry out cybercrime investigation in the cloud. Plus this, little work explains real case studies to illustrate the composite challenges related to cloud forensics in the real cases.

Little work was done to design and implement new models and systems to support cloud infrastructure investigation through giving the cloud system developer and architect, ideas of these new models to take them into consideration in the future during building novel secure and forensics support cloud infrastructure. This step can guarantee to public sectors who pose critical and sensitive data to migrate to the cloud. Thus, this chapter introduces the design and implementation of Cloud Forensics Investigation Model (CFIM) to investigate cybercrimes in the cloud environment.

The proposed system is an intelligent system that able to take a snapshot periodically for the state of each Virtual Machine (VM) which runs in the cloud and send it to Trusted
Center Server (TCS) that works as a storage for VM snapshots. The VM snapshot is very useful to a Cloud Investigators to analyze the VM to extract digital evidence to reconstruct the crime scene in the cloud. Snapshot also is significant because it is tricky with resuming the VM is that during the resume process, numerous files stored on the hard disk are altered, which may abolish evidence and thus the whole forensics process. The extra drawback of resuming the suspended VM is that there is a loss of information stored in the memory as the state of the VM changes. This information could be vital to the investigation being carried out. The TCS server also is responsible for monitoring and recording the status of the VMs. One of the important issues related to the proposed model. The use of this model should be mentioned as one of the terms in the Service Level Agreement (SLA) between Cloud User (CU) and Cloud Service Provider (CSP) to guarantee the success of the investigation process in the cloud through using this system integrated with cloud infrastructure in the future. The proposed system also introduced a real example of Forensics as a Service (FaaS) by including the FS in the CSP side for performing the digital investigation process through using the enormous capabilities of the cloud computing resources such as processing, computing, and storage.

7.2 Related Work

Cloud Forensics has become one of the imperative research areas in the cloud security domain. Performing the cloud forensics process poses many complex challenges due to the dynamic nature of cloud computing. Numerous researchers identified and explored various complex challenges facing digital investigators when performing cloud forensics and some of the proposed solutions for palliating these problems but still there are technical problems require being inspected.

Dykstra et al. [37], described the design and implementation of FROST for the OpenStack cloud platform. The FROST can help and assist the digital investigators and examiners to collect and acquire a virtual machine image with providing the integrity of this image with cryptographic checksums. This tool provides trustworthy forensic acquisition of virtual disks, API logs, and guest firewall logs. Unlike traditional acquisition tools. DeeviRadha and G. Geethakumari [76] proposed an efficient digital forensic investigation approach in cloud environment based on a Virtual Machine (VM) snapshots. The basic idea of this approach is that the Cloud Service Provider (CSP) stores snapshots of the VM whose
activities are identified as malicious using an Intrusion Detection System (IDS). Concurrently, the CSP should be requested for log files of the suspected VM and digital investigator collects and processes the log files to obtain the evidence.

Zafarullah et al [16] performed an experiment using Eucalyptus to monitor its behavior, in addition, to logging external and internal communication and interactions between components of the Eucalyptus. Type of attack called Distributed Denial of Services (DDoS) launched to simulate attacking scenario then they performed logging process. They were able to trace the DDoS attack. In [14], they suggested a cloud management plane for using in IaaS model where Cloud Service Providers (CSPs) can play an important role in data collection by providing a web-based management console. Using this console panel, users, and customers, as well as digital investigators, can collect and extract related digital evidence from virtual machine image, network, and process in an effective manner. There is only one problem with this solution is that it needs an additional level of trust in the management plane. In typical evidence, acquisition methods, where investigators have physical access to the system, this level of trust is not needed.

Zawoad, Shams, Ragib Hasan, and Anthony Skjellum [82], they introduced Open Cloud Forensics (OCF) model which considered the new role of the Cloud Services Provider (CSP) to support reliable and effective digital forensics in the cloud. They suggested that the proposed model can be used by cloud architects to design clouds that support trustworthy cloud architecture cloud forensics investigation. Simou et al [83] proposed meta-model for assisting the process of cloud forensics and moved present research one step further by recognizing the main concepts, actors, and their relationships that taking part in a cloud forensics process through the providing of their new meta-model. They also presented a running example, as well for better understanding the recommended concepts in related to cloud forensics investigation scenario.

Povar, Digambar, and G. Geethakumari [73] emphasized on the methods of finding and analyzing digital evidence in a cloud computing environment with respect to the cloud user as well as the provider. They proposed and introduced a heuristic model for carrying out digital forensics in the cloud environment. Their proposed model emphasized on the requirements of changes needed in data collection, preservation, and analysis of the digital investigation process. Dykstra et al [18] introduced a hypothetical case study of child
pornography to explain and illustrate the difficulty in the process of collection and acquisition of digital evidence. To prove the existence of contraband data about this case, digital investigators need to make copying or imaging process that bit-by-bit duplication of data. In the cloud environment, this process can do like confiscating the cloud server where many users store their data in the same storage of cloud.

In [26], Delport et al. studied how the isolation of an instance to mitigate the multi-tenancy issue. This isolation is necessary to help the investigators to secure and protect digital evidence from the violation. Hirwani, Manish, et al [84], they created a forensics snapshot analysis tool that needs that the two snapshots are of the same VM and the snapshots are converted to dd/raw format. The tool can then analyze the changes that have been made to the current snapshot by comparing these two snapshots. This tool analyses the changes made to a current snapshot of a virtual machine by comparing it to an earlier snapshot. When a VM is suspected of being compromised, a snapshot can be captured and this snapshot can be compared to a snapshot that is believed to be clean. This analysis can help in detecting new files added to or deleted from the virtual machine. The proposed tool does this by comparing the list of files found in the base snapshot and the list of files found in the compromised snapshot. Saad Alqahtany et al [85], they proposed an independent model to omit involvement of CSP. They used an agent-based approach that is held in each virtual machine and sending the required information to a central Cloud Forensic Acquisition and Analysis System (Cloud FAAs) in infrastructure as a service model.

The current literature has a dominant contribution in providing basic knowledge, new insight, vision, and ideas how to study cloud forensic and design some works but still, there are little mechanisms that implemented and have proof of concept for real cloud environments. Thus, authors in this chapter try to implement cloud forensics model as proof of concept to integrating the forensics process within cloud infrastructures to perform forensic investigation in an effective manner. Such kind of models could help the user or cloud service providers to identify the problem and in turn assist them to take automatic corrective action by applying the forensic investigation process with saving time and cost.

7.3 Proposed Cloud Forensics Investigation Model
Cloud Forensics pose numerous intricate challenges for performing the investigation process due to the dynamic nature of cloud computing to investigate cloud-based crimes and
reconstruct a crime event, then send a final report to a court of law as admissible evidence about the committed crime. In this part, we will introduce the proposed model which works to take snapshots of running virtual machines periodically through using Trusted Center Server (TCS) within a cloud architecture. This model can help tracking malicious users in the cloud environment in addition to, determine weaknesses of the running virtual machines for future use and finally provide support and help in the digital investigation process in the cloud. The basic idea is based on taking snapshots of Virtual Machine (VM) whose activities can be identified through monitoring and record them, then the Cloud Service Provider (CSP) can provide log files and related files about the suspected VM to digital investigators and examiners to obtain digital evidence about an incident that occurred in the CSP’s side. Then, performing the identification of the suspected VM, followed by moving or isolating to other locations to preserve confidentiality, privacy, and integrity of the remaining VMs which are running on the same cloud server. This step will provide protection of digital evidence from tampering or modification to be accepted in the court of law. Collecting the evidence in a proper manner can help the digital investigator to find the malicious users in the cloud.

7.3.1 Cloud Forensics Process
The cloud forensics process includes the following stages as identification, collection, preservation, analysis and finally presentation or documentation. During the presentation process, there is feedback to verify the digital evidence to ensure the integrity of it. Figure 7.2 shows the proposed cloud forensics process flow.

![Image of Flow Chart]

**Figure 7.2:** Flow of Cloud Forensics Process.

The verification of integrity can provide a feedback process as shown in Figure 7.2 due to the nature of volatile data in a cloud computing environment. This to protect and ensure the integrity of the digital evidence from manipulation and tampering. The verification
process can be done by the court of law on the evidence introduced by the digital investigators.

7.3.2 Malicious Scenario

In the cloud computing environment, the users can use cloud infrastructures for launching severe attacks. For example, the user can use his/her virtual machine to make illegal activities, in addition, to storing his/her illegal materials. This section introduces a malicious scenario to simulate what may occur on the cloud side. The malicious scenario can happen in the cloud like: John is cloud user who conducted Cloud Service Provider (CSP) of Amazon to create an account to register and use Infrastructure as Service (IaaS) for creating a Virtual Machine (VM). Another user called Alex rented VM for launching attacks and storing illegal materials such as photos and videos. Alex launched an attack against the VM of John to steal his data and also control it to use in launching Denial of Service (DoS) attack in the cloud environment. Then, John requested a digital investigator to investigate and find WHO attacked his VM. The investigator started to conduct the Amazon CSP to provide and help to collect any digital evidence related the incident of John’s VM.

In the above malicious scenario, there are several issues will meet the digital investigator during the investigation process. There are two scenarios in front the investigators may occur as follows:

- Alex can manage and handle to collude with the Cloud Service Provider (CSP) after the incident. The log files can be modified and manipulated by the CSP so that no way to verify the correctness of the logs. This context, lead to Alex will remain undetected.
- Even if the CSP was honest, Alex could finish and terminate the use of his VM. This lead no traces will be available to the investigators which make challenging in the cloud investigation process.

After the investigation process is completed, if the investigator does not discover the truth, in this case, the cloud user, John will be responsible for the committed incident on the cloud. To identify who made the malicious attack, there is a need to introduce new methods, techniques, or models to help the digital investigators and examiners in their mission of cybercrime investigation successfully in the cloud environment.
7.3.3 Cloud Forensics Investigation Model Components and Roles

This section provides a diagram for illustrating and explaining the investigation process in the cloud environment. The cloud forensics investigation model consists of five main elements which they play basic roles in this process. These elements are User(s), CSP(s), Attacker(s), Investigator(s) and the court of law as shown in Figure 7.3.

![Diagram of Cloud Forensics Investigation Model](image)

**Figure 7.3:** Digital Investigation Process in Cloud Environment.

Figure 7.3 shows the relations between the basic elements as well as the roles of them during the digital investigation process as follows:

1. **User(s):** Request a Cloud Services Provider (CSP) to create a Virtual Machine (VM) with specific descriptions.
2. **CSP(s):** Response to the user and create the VM then a direct connection between the user and the required VM will establish.
3. **Attacker(s):** Perform and launch severe malicious attacks.
4. **Investigator(s):** Remotely control in connection with the cloud side to collect and acquire digital evidence to make the investigation process and prepare a final report about crimes in the cloud environment.
5. **Court of law:** Responsible for adjudicate legal disputes between parties and carry out the administration of justice in civil, criminal, and administrative matters in accordance with the rule of law.
There are another three elements such as Incident, Cloud Services and Digital Evidence that have an important role in a cloud environment and performing the investigation process as follows:

1. **Incident**: In the cloud, it is occurrence or event that cause or perform illegal activities like attacks against cloud users or infrastructure.

2. **Cloud Services**: Means the services which provided by the CSP such as renting virtual machines and cloud storages.

3. **Digital Evidence**: It is the evidential data that extracted and collected from the cloud infrastructures such as log files to help the investigators for performing the investigation process. The digital evidence is considered as the proof about an incident that has occurred.

### 7.3.4 Forensics Investigation Model Supported Cloud Infrastructure

In the previous section, the investigation process in a cloud environment is introduced through defining the elements and roles of each element to understand this process and then propose new methods, techniques, and models. Based on the investigation model in Figure 7.3, we design cloud computing system, which is shown in Figure 7.4. This system works as an investigation model for supporting the cloud infrastructure in a forensically sound and timely manner. The proposed system called Cloud Forensic Investigation Model (CFIM).

We add to the previous model which illustrated in Figure 7.3 new elements such as a Trusted Center Server (TCS) and Forensic Server (FS). The TCS is an intelligent system that able to take a snapshot periodically for the state of each Virtual Machine (VM) which runs on the cloud servers and store them in related storage for supporting and providing the digital investigators with evidential data, in addition, to using for backup and recovery purposes.

The VM Snapshot allows automating the capture of plentiful pieces of information that are vital and critical during incident response and digital forensics. This information, including running processes, users on a system, network logs, open files and applications, Transmission control protocol (TCP) and User Datagram Protocol (UDP) port information. The other new component is the FS used to manage, handle and process the extracted and collected digital evidence, this can be done remotely by the digital investigator.

The use of FS supports the concept of Forensics as a Service (FaaS) that provide several advantages and benefits of conducting forensics process in the cloud environment side rather
than downloading the digital evidence in the investigator side which taking more time on delay in the investigation process. This delay in the time can delay the overall of the digital forensics process so that using the FS will help to benefit from the enormous capabilities of the cloud computing in performing the investigation process in a timely fashion way. To guarantee the success of the investigation process in the cloud through using this model, it should integrate the proposed model within the cloud infrastructure. Also, it is essential to mention this model in the Service Level Agreement (SLA) between Cloud User (CU) and Cloud Service Provider (CSP).

The proposed model provides the following features to support cloud forensics:

- Prevent loss of volatile data through recording snapshots of running VMs in a persistent storage.
- Help to issue a search warrant in respect of cloud environment through determining the location of TCS servers.
- No need to resume a suspend VM before the acquisition, which may potentially change the evidence through use VM snapshots.
- No need for large bandwidth to download an image of VM instance because the proposed model used the FS on the cloud side.
- Provide proactive strategy by preserving regular snapshots of VMs that can significantly help incident response and handling.
- Provide the Forensic as a Service (FaaS) concept through utilization of huge and massive computing and storage resources of cloud computing for performing the investigation process in a timely fashion manner.
7.3.5 Cloud Forensics Process Based on Proposed Model

After defining the elements and their roles in the proposed model supported cloud infrastructures as shown in Figure 7.4. This model can help in performing the investigation process. The complete investigation process based on the proposed model flowchart illustrated in Figure 7.5 as follows:

- The user requests a Virtual Machine (VM) with specific descriptions from CSP.
- The CSP response with the required VM and then the user uses it.
- Another user (Attacker) request a VM from the CSP.
- The CSP response to the user request and the VM created.
- In the background, Trusted Center Server (TCS) start to take periodically snapshot for running VMs.
- Hacking scenario occurred from the attacker to the user.
- After the hacking activity done, the user starts to conduct digital investigator to investigate this incident.
- The user sends a request to the digital investigator to investigate the committed incident against his/her VM.
• The digital investigator connects remotely to Forensic Server (FS) in the CSP side to request about the user VM.
• The FS request the TCS to send information about the attacked VM, then the TCS take permission from the CSP to provide the FS with the required VM.
• The TCS send the required VM's snapshots and Base Files to the FS for the investigation purpose.
• The investigator remotely will perform the investigation process phases which are identification, preservation, analysis, and presentation to reconstruct the committed crime event.
• A final report then generated about the committed crime.
• Finally, the investigator sends the report to the user or the court of law as admissible proof about the incident.

**Figure 7.5:** Cloud Forensics Process Flow Based on CIFM Model.
7.4 Implementation of Proposed Model

7.4.1 Experimental Environment

The experimental environment is setup using VMware products is prepared on laptop Lenovo G5080 Core i5 with 12GB RAM and Hard Disk 500GB, where VMware Workstation 11 installed on the host machine, then five virtual machines are created as the follows: ESXi-5 Server1, Domain controller, vCenter/ Trusted Center Server (TCS), Forensic Server (FS) and the investigator machine. Figure 7.6 shows the implementation of the proposed model. For the experimental purpose, in the ESXi-5 Server1, two virtual machines are installed. The first VM (VM1) assigned to cloud user and the second one (VM2) assigned to the malicious user (attacker), and a hacking scenario is launched from VM2 against VM1 to simulate a malicious activity in the cloud environment.

![Figure 7.6: Implementation of Proposed Model.](image)

7.4.2 Practical Scenario

In the cloud, various services can be provided by the cloud services provider to customers based on cost-per-use or some with the trial time that enables malicious criminals to perform malicious activities such as steal sensitive data of the customers in the cloud. Consequently, the cloud providers have to use protection and monitoring systems like Intrusion
Detection/Prevention System (IDS/IPS) and VM introspection to prevent these evil activities. Monitoring the behavior of VMs can be achieved through recording its snapshots. Snapshots are considered as a rich source of evidence for assisting the investigation to reconstruct and generate events [26]. The process of recording a VM snapshots is done through connecting to the ESXi server then store it with the VM files in the Datastore. The forensic server then requests the VM files included snapshot files to start the forensic investigation process. Finally, a forensic report generated by the digital investigator. The general procedure to do this process is shown in Figure 7.7 as follows:

1. Start record snapshots of specific VM.
2. The recorded snapshot will store in datastore with other VM files hosted on the ESXi server.
3. The forensic server requires the specific VM files to start forensic investigation process.
4. Using transfer strategies like vMotion of VM to transfer VM files from datastore to the forensic server.
5. The investigator starts remotely performing forensic investigation process.
6. The final forensic report will be generated after finishing the forensic investigation process.

![Diagram](image)

**Figure 7.7:** Taking Snapshot and Forensic Analysis of Specific VM.
For the research purpose in this chapter, the practical procedure performed as follows:

1. Start recording and take snapshots for VM1 and VM2.
2. The recorded snapshot will store in the datastore of ESXi server.
3. Launch the hacking scenario from VM2 “Attacker” with IP Address: 10.10.2.101 to VM1 “Victim” with IP Address: 10.10.2.100.
4. Start recording and take snapshots for VM1 and VM2.
5. The recorded snapshot will store in a datastore of ESXi server.
6. The forensic server requires the VM1 and VM2 files for the forensic investigation purpose.
7. Using transfer strategies to transfer VM from datastore to the forensic server. (i.e. Download VM files)
8. The digital investigator starts remotely performing forensic investigation process.
9. The final forensic report will be generated after finishing the forensic investigation process.

7.4.3 Results Analysis and Discussion

Before the implementation of the proposed model, we faced two problems. The first one, how the digital investigator will perform the investigation process using Forensic Server (FS) remotely and the second one is how the Trusted Center Server (TCS) record and take snapshots of running Virtual Machines (VMs) on VMware ESXi server. For the first problem, the digital Investigator can use the Remote Desktop Program (RDP) like on Windows operating system to remotely connect to the forensic server and perform the investigation process where digital forensics tools are installed. The Remote Desktop Connection Program for Windows is shown in Figure 7.8. In the computer part, the investigators write the IP address or domain name of the forensic server then will request a password for authentication purpose to prevent unauthorized users from accessing it.
Figure 7.8: Remote Desktop Connection Program.

For the second problem which represents the basic idea is taking a snapshot of running VMs. Most virtualization products like VMware’s ESXi providing snapshot capability of running virtual machines. A VMware snapshot is a point-in-time image of a VM, including volatile data from Random Access Memory (RAM) and the virtual machine disk file. The resulting file can provide digital investigators with an encapsulated copy of the machine at the time when the breach or malicious activity occurs. Also, the snapshot of VM enabled the investigators to capture the entire state of the virtual machine at the time it is snapshotted. It is useful to revert repeatedly to the same state without having to create new virtual machines. The snapshot contains several vital information such as settings of the virtual machine, the state of all the virtual machine’s virtual disks and memory contents of the virtual machine that represent volatile data. VM Snapshots allow preservation of evidence. Seizing the related files and taking them to a secure forensics location is easily accomplished. For implementing the proposed model, there are several solutions to take snapshots of VM such as follows:

1. To use vmrun command-line utility involved with the VIX API libraries. The vmrun utility enables administrators to control the running virtual machines in VMware product platforms, including VMware Fusion, Workstation player, VMware sphere, and VMware servers. This utility uses to perform various tasks on virtual machines such as Snapshot captures and record virtual machines events as follows [86]:

   - **Snapshots Capture:** Capture the virtual machine state at the time of the snapshot, containing all data on virtual disks. It possible to take a snapshot of a virtual machine
in any power state and revert to the snapshot at any period. Snapshot commands can list existing snapshots of a virtual machine, create a new snapshot, delete a snapshot, and revert a virtual machine to its state as of a specific snapshot. VMware Server limits you to one snapshot. For example, the following command shows take snapshot of virtual machine with VMware Workstation on a Linux host: “vmrun -T ws snapshot /path/to/vm/Ubuntu/Ubuntu.vmx mySnapshot”

- **Record and Reply:** The recording is named a snapshot object but is really more like a movie. At the moment, only VMware Workstation supports record and replay. These commands begin or end the recording of events, and begin or end the replay of a recording. For example, the following command explains start recording user events on a Windows guest, starting with a snapshot of virtual machine state: “vmrun -T ws -gu <user> -gp <pass> beginRecording WinXP\WinXP.vmx session1”

2. To use the command line on ESXi host to capture a snapshot of virtual machines. The following command explains how to take a snapshot of a virtual machine that runs on ESXi host: “vim-cmd vmsvc/snapshot.create [VmId] [snapshotName] [description] [includeMemory] [quiesced]” where the [includeMemory] and [quiesced] variables are boolean values. Set the value to 1 to enable or 0 to disable the snapshot option. For example, create virtual machine with name ‘my_snapshot’, description is ‘snapshot_test’ and the value of ‘includeMemory’ and ‘quiesced’ is 0 as follows: “vim-cmd vmsvc/snapshot.create 10 my_snapshot snapshot_test 0 0”

3. To write a PowerShell script to take periodically snapshot of the running virtual machines on the ESXi server. In the Windows, PowerShell script will write a description of the virtual machine and path to Datastores where it's stored and finally the path to the destination where the virtual machine files will store. PowerShell script can use to take snapshot from one or multiple virtual machines as follows:

- **Create Snapshot for one Virtual Machine:** The following command illustrates of calling the snapshot name “Snapshot_1”. Replace “VMname” with the name of your VM and “Snapshot_1” with the name you would like to call the snapshot. After the command completes, a snapshot of the virtual machine with the specified name will be created. Note that the time required for completing taking a snapshot of the virtual machine will vary depending on the size of it. The command of creating a snapshot
for one virtual machine is: “Get-VM VMname | New-Snapshot -Memory -Quiesce -Name Snapshot_1”

- **Create Snapshot for Multiple Virtual Machines:** For creating a snapshot of multiple Virtual Machines (VMs) with each Snapshot will be named “Snapshot_2”. In the case of using vCenter for easy management of the ESXi severe where the VMs organized by folder in the vCenter.it has easily taken a snapshot of all VMs in the folder by specifying the location. The following command taking snapshots of all virtual machines located under the “Folder1” folder: “get-vm -location “Folder1” | New-Snapshot -Memory -Quiesce -Name Snapshot_2”

4. Another solution, we proposed an application that can help the digital investigators to take snapshots of the virtual machine and extract useful information like a number of files created within the virtual machine and information about the storage system of the ESXi host. Figure 7.9 shows the functions that the proposed application can provide on VMware ESXi host. This application is a simple step to developing new forensics tools that can work with VMware products like ESXi for the investigation purpose. As shown in Figure 7.9, “Virtual Machine_1” is a virtual machine running on the ESXi host during the test of the proposed application.

![Virtual Machine Forensics Page](image)

**Figure 7.9:** Take Snapshot of Virtual Machine using Forensic Application.
Virtual Machine Acquisition: The acquisition process of the virtual machine is a significant step in performing the forensic investigation process due to all next stages will depend on it. In a virtualized environment, data for a virtual machine are stored in the storage area on a server and not on the local system like in Personal Computer (PC) and mobile phones. This led the digital investigators to investigate the storage area which includes multiple independent storage devices so that it will be difficult for them to collect and acquire data from these storage devices. The solution for this problem is to acquire a virtual hard disk of the virtual machine. However, it is difficult to acquire data for a virtual machine because the virtual hard disk can be allocated in various ways: a single or multiple files and via static or dynamic allocation. The data could be stored on one physical disk or distributed across multiple disks. Therefore, we use the hypervisor management system and shell connection program to acquire a virtual hard disk of the suspect user.

Doowon Jeong et al [75] proposed a digital investigation approach for Virtual Desktop Infrastructure (VDI) solutions. They focused on a virtual desktop infrastructure and presented several desktop virtualization solutions that are commonly used like Microsoft, Citrix, and VMware. They illustrated and introduced methods for data acquisition of virtual machines through two ways which are, hypervisor management system and shell connection program as follows:

- **Hypervisor Management System:** Here, we focus on VMware hypervisor management system which called vCenter for acquiring virtual machine through exporting or duplicating in addition to downloading VM files. Data acquisition and collection methods for virtual machine data using the hypervisor management system from VMware (i.e. vCenter) as shown in chapter 5 in Table 5.2.

- **Shell Connection Program:** VMware provides a Command-Line Interface (CLI) with various administrative and management-oriented utilities. One such utility allows acquisition of a copy of the state of the virtual machine. VMware can collect the raw data duplicated from the original virtual disk. VMware provides a method for collecting virtual machine data using the shell connection program as follows: Connect to the shell using vSphere PowerCLI Virtual disk collection command: copy-datastore item [datastore drive]:\[Source Path] [Destination Path].
Any virtual machine has several states such as running, suspended, or in a power-off state. Before data acquisition, the digital investigator should check the state of the virtual machine due to the acquisition method that is applicable varies, depending on its state, so that it is better for the digital investigators to understand which methods are suitable to facilitate the forensics process and save time. Table 7.1 shows the applicable acquisition methods with state of the virtual machine.

**Table 7.1: Data Acquisition Methods with State of Virtual Machine [75].**

<table>
<thead>
<tr>
<th>Acquisition Method</th>
<th>Running</th>
<th>Suspended</th>
<th>Turn off</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM export</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VM duplication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VM configuration file download</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI program</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Forensic Analysis of Virtual Machines and Their Snapshots:** In a forensic analysis of virtualized environments, when the investigators working with suspended virtual machine images, they have two choices for acquiring the virtual hard disks - either resuming the suspended machine, then use bit-by-bit copy or to directly work with the virtual machine files. The problematic with resuming the VM is that during the resume process, numerous files stored on the hard disk are altered, which may abolish evidence and thus the whole forensics process. The extra drawback of resuming the suspended VM is that there is a loss of information stored in the memory as the state of the VM changes. This information could be vital to the investigation being carried out. So that, in this chapter, authors focus on using snapshots of the running virtual machines in the virtualized environments such as cloud computing that can overcome the drawback that pointed out above. In this research, after taking and recording snapshots of the user and suspect virtual machine, the TCS send it and related files to the FS to start the investigation process remotely by the digital investigators. In the FS, several important forensics tools are installed for performing the investigation process in an effective manner. These tools such as AccessData FTK Toolkit, Encase, and Autopsy. Finally, a forensic report will generate to document the incident events in the cloud.
environment and send it to the cloud user or court of law as admissible proof about committed crime.

For the research purpose, the authors used the vCenter as Trusted Center Server (TCS) to perform the function for both at the same time so it can benefit from the vCenter capabilities of taking periodically monitoring of the virtual machines in the one or multiple ESXi servers and the normal role for management of ESXi servers. In the experimental environment, after recording a snapshot of VM1 and VM2. The investigator started downloads the files of them to perform the forensic analysis process in the FS remotely. For each virtual machine, two snapshots are generated first one before hacking and the second after. In the beginning of the forensic analysis, forensic raw images from the virtual machine hard disk and their snapshots are created using FTK imager tool with calculating the hash values for them without relying on write blockers. This methodology of creating hash values to ensure the integrity of digital evidence as well as guarantee the process is forensically sound. Using memory forensics analysis tools as Volatility Framework - Volatile memory extraction utility framework [87], which use to the extraction of digital artifacts from volatile memory (RAM) samples or memory dump for a VMWare Virtual Machine ‘.VMSN’ file. For the victim or user machine, the two snapshots files are analyzed using the aforementioned tool using following commands to extract image information, process list, and network connections as follows respectively:

1. C:\Python27\volatility-master>python vol.py imageinfo -f Path of VMSnshotFileName.vmsn
2. C:\Python27\volatility-master>python vol.py pslst -f Path of VMSnshotFileName.vmsn
3. C:\Python27\volatility-master>python vol.py connscan –f Path of VMSnshotFileName.vmsn

The output of memory analysis proof that there is a connection between the attacker machine and victim machine through the port 4444 that commonly used as the default listener port [88] for the Metasploit framework as shown in Figure 7.10. This means that the attacker may use the Metasploit framework for launching attacks against the user inside ESXi server. Figure 7.11 shows the output of memory analysis for process list where noticed that the use of a cmd.exe process that used by an attacker to control the victim system. The next step is to the analysis of hard disk of both machines of the victim and the attacker with IP Address ’10.10.2.101’ to extract and confirm the criminal activities of the attacker against the user with IP Address ‘10.10.2.100’. From Figure 7.10, observed that there is a connection
established between the victim and attacker as a proof to help the investigators to identify which machine launched the hacking.

<table>
<thead>
<tr>
<th>Offset(P)</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>Pid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01706628</td>
<td>10.10.2.100:1037</td>
<td>10.10.2.101:4444</td>
<td>1092</td>
</tr>
<tr>
<td>0x01af4e70</td>
<td>10.10.2.100:1035</td>
<td>10.10.2.101:4444</td>
<td>1092</td>
</tr>
</tbody>
</table>

**Figure 7.10**: Output of Memory Analysis for Network Connections.

Before the hacking scenario done, the user did some activities such as snapshot created, create file1.txt, file2.txt, and file3.txt, then delete file3.txt, and finally create bitmap image called image1.bmp. After that the hacking scenario did as follows:

- Run Metasploit framework to start the hacking process.
- Create a screenshot of victim machine.
- Control the shell of victim machine and do some activities such as create text1.txt, text2.txt, then delete text2.txt
- Perform key logging while the victim writing on notepad in desktop and record and save it as dump1.txt.
- Upload to “C:\” in victim machine, which a screenshot picture for the victim machine taken by the attacker. This image name is “PJEMVKZY.jpeg”
Used TightVNC program to monitor screen of victim machine.

Denial-of-service Attack - DOS using hping3 10.10.2.100 –flood.

**User/Victim Machine Analysis:** First step in the forensic analysis of any system creates an image of it. Using FTK imager tool, an image created for the victim machine included snapshots. As known in digital forensics field, it must check the integrity of the digital evidence (image) using cryptographic hash algorithms such as MD5 and SHA1. Hash values for the images created and matched. AccessData FTK Imager v3.4.2.6 and Guidance Software EnCase v6.18 software are used to analyze the user machine to extract any proof related to the aforementioned criminal scenario. It was observed that three files and one image in the user machine which are created by the user in the Desktop as shown in Figure 7.12. Also found links files for them when analysis using Encase as shown in Figure 7.13. Figure 7.14 shows file3.txt in Recycler which is deleted by the user. One criminal activity that done by the attacker, was capture screenshot of victim system through using the console to control his system, then uploaded it to the victim machine. The screenshot name is “PJEMVKZY.jpeg” as shown in Figure 7.15. Another activity done by the attacker is created text1.txt file during using the console which found a shown in Figure 7.16.

**Figure 7.12:** Files Created by the User in Machine Desktop.

**Figure 7.13:** Links to the Files Created by the User.
To measure the performance of the user machine during the DOS attack, screenshots captured to CPU and NETWORK performance before and during the attack as shown in Figure 7.17 to Figure 7.20. The change in the CPU and Network performances refers to illegal or criminal activity was occurring. This can help in the future with help of Intrusion
detection systems to develop methods and procedures to perform forensics automatic according to changing in the system performances, which can reduce time and cost of the digital forensic process.

![Figure 7.17: CPU Performance before DOS Attack.](image)

![Figure 7.18: CPU Performance during DOS Attack.](image)
**Criminal/Attacker Machine Analysis:** Here, after creating an image for the attacker machine using FTK Imager and hash values matched, the analysis process done using autopsy forensics tool. From the analysis was observed the screenshot in the attacker machine as shown in Figure 7.21. Also observed there a screenshot image of attacker system during using TightVNC program to control the victim machine as shown in Figure 7.22.
**Figure 7.21:** Screenshot of Victim System Found in Attacker Machine.

**Figure 7.22:** Screenshot of Attacker Machine while using TightVNC Program against Victim Machine.
From the analysis of digital evidence related to the criminal/hacking scenario that aforesaid for the research purpose between both victim and attacker machines, found that there is an admissible proof that machine with IP Address ’10.10.2.101’ is responsible for the crime in the cloud that occurred against the user machine with IP Address ’10.10.2.100’, thus conclude that the proposed model can assist and help digital investigators and examiners to reconstruct crime events in cloud computing environments with efficient, forensically sound and timely effective manner.

---

**Final Forensic Report for Investigation attacks in Virtualized Environment**

1. **Case Number:** 20161210-001-CloudCrime.
2. **Examiner:** EZZ.
3. **Status:** Finished and completed.
4. **Crime Scene:** Cloud Computing Environment.
5. **The conclusion of Findings:**
   - Screenshot image related to the victim machine.
   - Network connection established using port 4444 between Victim Machine and attacker.
   - Text1.txt file creates by attacker founded in victim machine.
   - Screenshot image of attacker system during using TightVNC program to control the victim machine.
   - Noticed changing in CPU and Network performance during DOS attack.
6. **Items analyzed**
   - Two virtual machines, “Windows XP and Kali Linux” with their snapshots, which acquired from ESXi Server.
7. **Details of Findings:**
   The findings related to virtual machines hosted by ESXi server are:
   - The analyzed virtual machines were found contains Windows XP and Kali Linux operation systems.
   - Screenshots for the victim machine and 4 for the attacker machine.

**Written By Examiner:** EZZ  
**Date:** 11-12-2016

### 7.5 Chapter Summary

Several researchers explored and identified various complex challenges facing digital investigators when performing cloud forensics and some of the proposed solutions for palliating these problems but still there are technical problems require being inspected. This
chapter introduced the design and implementation of a new cloud forensics model which is called ‘Cloud Forensic Investigation Model (CFIM)’. The implementation of the proposed model within cloud architecture can increase the probability of tracking malicious users in the cloud environment, determine weaknesses in cloud services such as virtual machines for future use as well as support cloud forensics investigations in forensically sound and timely fashion. The proposed system provided several benefits to support cloud forensics such as:

- Prevent loss of volatile data through recording snapshots of running VMs in a persistent storage.
- Help to issue a search warrant in respect of cloud environment through determining the location of TCS servers.
- No need to resume a suspend VM before the acquisition, which may potentially change the evidence through use VM snapshots.
- No need for large bandwidth to download an image of a virtual machine instance, because the proposed model used the FS on the cloud side.
- Provide proactive strategy by preserving regular snapshots of VMs that can significantly help incident response and handlers when the incident occurs.
- Provide the Forensic as a Service (FaaS) concept through utilization of enormous computing and storage resources of cloud computing for performing the investigation process.
- Ability to identify the criminals and attackers inside the cloud environment.