Chapter 6: HFAA: A New Forensic Application for Acquisition of Digital Evidence from Clustered VMware ESXi Hypervisors

Virtualization plays a significant role in the development of IT industry. The virtualization technology, introducing several merits for organizations such as cost benefits through a decreasing number of physical machines required within an environment as well as best utilization of hardware resources such as storage, processing and computing resources. Nevertheless, the digital forensics community appears a little bit slow in this theme. Therefore, current forensic techniques and tools cannot cope with virtualized environments. There is some research work available with a general understanding of the mechanisms of virtualization, but not on how to forensics acquisition and analysis of digital evidence from it. Especially, large clusters of hypervisors which are sharing virtual machines and storage distributed across IT infrastructures.

To contribute solving part of this problem, this chapter aims to propose a new forensic application called Hypervisor Forensic Acquisition Application (HFAA) for acquisition and extraction of digital evidence from clustered VMware ESXi hypervisors for helping digital investigators and experts in performing the digital investigation process. The proposed system is built on top of open source Virtual Infrastructure (VI) Java Application Programming Interface (API), which is built on top of the Web Services API. Using this API instead of Web Services can give much shorter, faster, and more readable code. This application utilizes this feature to provide full control to manage and handle vCenter/ESXi for performing incident response and digital investigation. The proposed application is an initial step and a guide for digital investigators and researchers to develop new approaches and methods for acquisition, extracting and analysis of digital evidence from the clustered VMware ESXi servers in forensically sound and timely manner.

The rest of this chapter is structured as follows: section 6.1 discuss an introduction to the prominence of virtualization technology as well as challenges to the investigation of
crimes in clustered VMware Hypervisors while VMware virtualization technology is provided in section 6.2. Section 6.3 presents related and previous work while the proposed system with results analysis, evaluation, and limitations are presented in section 6.4. Finally, the chapter summary is introduced in section 6.5

6.1 Introduction

In recent times, virtualization technology is becoming very popular technology due to it plays an important role in IT community and industry to overcome physical limitations in hardware. The virtualization technology provides a lot of benefits that includes management flexibility and best utilization of processing, computing, and storage hardware resources. This enables to save cost and time for IT enterprise.

The desktop virtualization is one of the virtualization technologies applies the resource of a host by allocating it as multiple logical resources and can operate a guest operating system on a host operating system. The representative vendor that leads such a desktop virtualization technology is VMware, which first released a virtualization product based on an x86 server platform in the market.

A virtual machine is a collection of applications, operating systems, and virtual hardware resources which works as a physical system. Since the virtual machine can achieve the same role as a physical system, therefore it possible to record a user’s activity in a virtual machine. Recording the user’s activity trail in the virtual machine is significant digital evidence for digital forensics. The VMware hypervisors such as VMware Workstation or VMware ESXi, as the default creates each virtual machine image, memory dump, configuration, and log file. Therefore, these files can be used for the forensic purpose. However, there are few specific studies on the investigation method. Moreover, a user’s intentional act or process of collecting images can incur damage to the virtual machine’s files. Because it is tough to investigate the clustered ESXi hypervisors, the relevant research is needed for collect and analysis of the digital evidence which can be acquired from them.

This makes forensic experts and researchers think to solve this problem through design and develop new tools because traditional forensics tools cannot cope with an acquisition and analysis of digital evidence from virtualized environments. We focus on this research on VMware ESXi hypervisor, which is considered one of the most hypervisors, which can
be clustered to distribute and share a virtual machine and storage. Therefore, it is adopted by several organizations as an efficient and cost-effective solution for IT infrastructures.

VMware provides virtual infrastructure management software such as sphere client, which enables to manage virtual datacenter, but that may be not suitable for forensics purpose because the vSphere client allows to system administrators to perform full administration of virtual datacenter. Consequently, we start thinking how to develop an application similar to the vSphere client, but for cybercrime investigation in a virtualized environment without breach privacy and security of users in the data center. This can be done by designing an application with limited privilege for digital investigators to protect the privacy and security of virtualized environment users. Therefore, in this research, we suggest a forensic acquisition application called Hypervisor Forensic Acquisition Application (HFAA) for the acquisition of digital evidence from clustered VMware ESXi servers. Through these, the investigator will be able to carry out an appropriate forensic investigation on virtual machines and obtain meaningful data from the ESXi servers.

The proposed system is built on top of open source Virtual Infrastructure (VI) Java Application Programming Interface (API), which is built on top of the Web Services API. Using this API instead of Web Services can give much shorter, faster, and more readable code. Therefore, this application an alternative approach for the acquisition of evidence data from virtualized environments through utilizing this feature to provide full control to manage and handle ESXi servers for performing incident response and digital investigation. This application can assist digital investigators and experts in performing the digital investigation process where the virtual data center is used in the cloud computing environment. The proposed application can be considered as an initial step and guide for digital experts and researchers to develop new approaches and methods for acquisition, extracting and analyzing the digital evidence from the clustered VMware ESXi servers in forensically sound and timely manner. The design of proposed system supports to scale in a dynamic nature of virtual environments such as cloud computing, where distributed clusters of hypervisors for providing better and on-demand computing services.

The HFAA capabilities have been validated in a small yet realistic experimental environment. The application connects to an ESXi server (s), to extract digital evidence such
as VM snapshots that contain recording a user’s activity trail in the virtual machine, information about storage of hypervisors, log files of VM, OVF of VM as well as control VM operation like power on, power off and suspend it. These capabilities can assist in digital forensics. The application securely extracts information related to the selected virtual machine running on a VMware ESXi hypervisors and also can export OVF file that contains a virtual machine’s hard disk with ensuring data integrity through generated hash values for the entire exporting process. With some additional development and testing in a larger environment, this could potentially become the go-to tool used to acquire images from VMware ESXi hypervisors.

6.2 VMware Virtualization Technologies

The virtualization technology which plays an important role in the development of IT industry. With the increasing demand for computing services, the virtualization has revolutionized the data centers operation around the globe. This enables users to run multiple Virtual Servers or Virtual Machines (VMs) in the same single physical server to reduce costs and best utilization of available hardware resources.

A virtualization manager which create, manage and monitor virtual machines called Hypervisor or Virtual Machine Manager (VMM), which simulates pool of physical hardware such as hard disk, processor, memory, and other hardware components and software which needed for each virtual machine. The hypervisor has several characteristics such as the hypervisor has full control of managing and monitoring system resources, providing an environment for programs to run as running on the physical machine and these programs that work in this environment have very small speed degradation compared with the physical machine (i.e. host machine). There are two types of hypervisors which are Bare-metal and hosted based hypervisor as follows [2][5]:

6.2.1 Bare-metal Hypervisor

The Bare-metal Hypervisor straight operates on a physical hardware system as shown in Figure 6.1 and does not need a host operating system. As it installs directly on top of the physical machine and has direct access to resources, this makes its performance comparable to that of native execution. Also, due to it does not essential to allocate resources to a host operating system, this type of hypervisors represents a small overhead compared with the
Hosted based hypervisors and a flexible management in the resources of physical computers. The representative Bare-metal Hypervisor virtualization tools from VMware are ESX and ESXi servers and vSphere platform, which is an enterprise product based on these servers.

6.2.2 Hosted-based Hypervisor

The Hosted based hypervisor runs on top of an already installed standard operating systems such as Linux, Mac, and Windows as shown in Figure 6.2. Although this type shows large overheads because it emulates such hardware, it has been basically used in x86 desktops because of the fact that it has no limitations in guest operating systems. The representative Hosted based hypervisors tool of VMware is the VMware Workstation.

![Figure 6.1: Bare-Metal Hypervisor.](image1)

![Figure 6.2: Hosted based Hypervisor.](image2)
In keeping with the growth in the use of virtualization solutions by enterprise and private users, the need for the investigation of virtualization environments is increased. For implementing a digital forensic investigation for the virtualized environment, it is essential to understand how this virtualization environment is planned, where data is stored, and which files represent important meanings. The structural of virtual environments is different from physical environments so that it is better for digital investigators to understand the files associated with a virtual machine. This can help to provide good investigation results during acquisition and collection of digital evidence.

Table 6.1 shows the key files for configuring a virtual machine which are .vmx, .vmdk, .nvram, .vmsd, and .log. The main files of the investigation in the forensic aspect are .vmx, .vmdk, .vmem, and .log. Besides, the VMSD and VMSN files which are can play a significant role in a recovery point of a virtual machine, and the VMSS file that stores the state of a suspended virtual machine involve the virtual machine snapshot, it is necessary to implement additional investigations. The description of these files as follows:

- **VMX File:** It stores the configuration information chosen in the creation of a virtual machine. The configuration information involves an encoding method, a virtual disk connection manner, the information of connected virtual devices, and the size information of the configured disk. This file can be used to verify the overall information of the virtual machine because of it comprises most of the configuration information.

- **VMDK File:** It is a binary file that plays a role in a virtual disk of a virtual machine and configures the virtual machine image. It can allocate the VMDK file as much as the configuration size of a virtual machine and increase it dynamically. Also, it can implement management work by dividing it into multiple VMDK files with a unit of 2 GB. The VMDK file contains a large amount of data, which represents meanings in the forensic aspect.

- **VMEM File:** It is a binary file that stores the memory data of a virtual machine and exists as the virtual machine is being operated in a suspended state. The VMEM file performs a back-up of the memory of a virtual machine which is being operated, and
the backup memory will be automatically deleted as the operation of the virtual machine is terminated. Besides, as a virtual machine is terminated as a suspended state, the data will remain.

- **LOG File**: It stores the activity information of the VMware Workstation that operates a virtual machine as a text format. As a problem or error in the operation of a virtual machine occurs, the reason of the problem or the error can be fixed through the LOG file. The LOG file contains the configuration information that is not stored in the VMX file. Thus, it should be checked in a verification process for the information of a virtual machine together with the VMX file.

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.VMX</td>
<td>It stores setting and configuration information of a virtual machine.</td>
</tr>
<tr>
<td>.VMTM</td>
<td>It contains configuration information containing the specific group data of a virtual machine. A team is a group of virtual machines which can inter-operate in a VMware virtual environment.</td>
</tr>
<tr>
<td>.VMXF</td>
<td>It stores configuration information remained as the specific group is deleted.</td>
</tr>
<tr>
<td>.VMDK</td>
<td>It represents configuration files of a virtual hard disk, which may be either dynamic or fixed virtual disk.</td>
</tr>
<tr>
<td>.LOG</td>
<td>It contains a log of activity on a virtual machine or a hypervisor.</td>
</tr>
<tr>
<td>.NVRAM</td>
<td>It stores Bios state information of a virtual machine.</td>
</tr>
<tr>
<td>.VMSS</td>
<td>Information of a virtual machine at a suspended state.</td>
</tr>
<tr>
<td>.VMSN</td>
<td>It stores snapshot information of a virtual machine.</td>
</tr>
<tr>
<td>.VMSD</td>
<td>It contains snapshot metadata of a virtual machine.</td>
</tr>
<tr>
<td>.VMEM</td>
<td>It is a backup of the virtual machines aging files of a virtual machine or storing the entire memory.</td>
</tr>
</tbody>
</table>
6.3 Related Work

Recently, the rising usage of cloud computing and increasing utilization of cloud resources, services and technologies are forcing the development of virtualization technologies like VMware products. With cloud computing on the ascension, the crimes using and against cloud and virtual environments are increased, therefore, there is even a demand to be able to conduct digital forensics on virtual infrastructures such as hypervisors and virtual machines or appliances that exist in the cloud systems.

A number of researchers have attracted attention to the fact that not much research has been performed in the field of cloud forensics and question if traditional forensics tools and methods can be applied to conduct forensics on the cloud. A literature study on the forensic acquisition and analysis of clustered VMware ESXi hypervisors resulted in very few information to that specific matter. However, there was some research work related to the subject.

Hirwani securely acquired the virtual hard disk file and corresponding snapshots from a VMware virtual machine. After getting hold of these digital forensic images, they were analyzed by a program developed by Hirwani that compared the snapshot files to determine what files had been created, deleted, or modified [77]. Research has also been done to evaluate using a virtual environment to conduct forensic analysis. After acquiring a digital forensic image from the suspect machines hard drive, it is converted into a virtual machine, allowing an investigator to boot the machine and perform digital forensics without affecting the original evidence [78].

Martini and Choo developed a six-measure procedure to gather digital evidence from a cloud platform, utilizing VMware vCloud as a case study. In summation, a proof-of-concept program was created that made use of clouds Representational State Transfer (REST) Application Programming Interface (API) to acquire digital forensics information following their proposed process [79].

To ease and simplify the acquisition of digital evidence from VMware ESXi servers, there was a need to streamline the process and remove the likelihood of human errors during evidence collection. A program named ESXimager which was created using the Perl
ESXimager gives a forensics investigator a simple yet strong means of acquiring digital evidence from VMware ESXi hosts [80]. The existing literature has a paramount contribution in providing basic knowledge like there are numerous tools dedicated to conducting digital forensics that is both open source and proprietary. Despite the number of forensic tools available, a specific niche has yet to be filled that gives forensics investigators the ability to rapid acquire and collect digital evidence from clustered VMware ESXi hypervisors which are distributed to share virtual machines and storage so that this chapter introduces the design and implementation of HFAA- a Hypervisor Forensic Acquisition Application for clustered VMware ESXi hypervisors that can be used to build virtual environments.

6.4 Proposed System
This section describes in details the architecture, flowchart and implementation of the proposed system that aims to help digital investigators and practitioners for performing acquisition of clustered VMware ESXi Servers in a timely fashion and forensically sound manner.

6.4.1 Architecture of Proposed System
The proposed system is built on top of open source Java API [81], which is built on top of the Web Services API. Using this API instead of Web Services, Forensics developers can have much shorter, faster, and more readable code.

In this research, we utilizing this new feature to build the proposed system to provide full control to manage and handle vCenter/ESXi for performing incident response and digital investigation in effective and efficient manner. The architecture of the proposed system is shown in Figure 6.3, where the proposed application is built on top of the VI Java API layer to providing fast and rapid response and performance in digital forensics.
Figure 6.3: Architecture of Proposed System.
6.4.2 Flowchart of Proposed System
The steps of using the proposed system for accessing and acquiring forensics data from clustered ESXi servers is explained in the following flowchart as shown in Figure 6.4

![Flowchart of Proposed System](image)

Figure 6.4: Flowchart of Proposed System.

6.4.3 Implementation of Proposed System
The proposed system is built using Java programming language because Java is a popular programming language that runs on all major platforms and has the widest audience today. Also, The Java has many features which can be used to develop large-scale applications in different domains. The proposed application is based on VI Java API that helps us provide full control to manage and handle vCenter/ESXi servers.

6.4.4 Experimental Environment
In order to evaluate and test the use of the proposed HFAA- a Hypervisor Forensic Acquisition Application, an experimental environment is created to represent a small-medium enterprise that use of clustered VMware ESXi servers. Due to the cost of implementing of virtualized environments, The experimental environment is set up using Laptop Lenovo G5080 Intel(R) Core(TM) i5-5200U 2.20 GHz, 12GB RAM with Hard Disk
500GB. VMware Workstation 11 is installed on the host machine then five virtual machines are created as follows: two ESXi 5.5.0 Servers, one Windows Server 2012R as Domain Controller and one Windows Server 2012R as vCenter Server and one Windows 7 Machine as a Developer device. Within the first VMware ESXi 5.5.0 server, three more virtual machines are being run while in the second VMware ESXi 5.5.0 server, two more virtual machines are being run. In the developer device, Java eclipse is installed as editor for writing the proposed application using Java programming language. These five virtual machines share the host machine’s Ethernet adapter, which allows each virtual machine to logically appear on the same network. The experimental environment is built as shown in Figure 6.5. The objective of this experiment is:

- To test the functionality of the proposed application to acquire digital evidence from two clustered VMware ESXi hypervisors as shown in Figure 6.5.
- To evaluate the performance of the proposed application with existing programs like VMware vSphere client.
- Check integrity of acquired digital evidence to be admissible for providing in a court of law.

![Diagram](image)

**Figure 6.5:** Topology of Experimental Environment.
6.4.5 Results and Application Use
This part explains the use of the proposed application to extract valuable information from VMware ESXi hypervisor that can help digital investigators in performing the digital investigation process. To use the proposed application, the investigators have to install it in their machines to connect to a cluster of ESXi servers. A generic view of the investigator’s interaction with the virtual datacenter is shown in Figure 6.6.

![Diagram of Remote Data Acquisition from Virtual Datacentre Using Proposed System](image)

**Figure 6.6:** Remote Data Acquisition from Virtual Datacentre Using Proposed System.

1. **Login Page:** Important part in any application is the Graphical User Interface (GUI) which is preferred more than a command line is driven approach because it makes the application more user-friendly through allowing for information to be easily and clearly displayed, and allowing the user to easily interact with the application’s many features. HFAA utilize the feature in Java to build GUI elements. The look and feel of the application when it is first run login page as shown in Figure 6.7. The user has to fill this login Page with IP Address, Username, and Password to access the ESXi/vCenter server. The HFAA GUI has a number of different features; the purpose and functionality will be explained below.
Figure 6.7: Login Page to Access ESXi/vCenter Server.

2. **Select the Virtual Machine**: After the user is login to the ESXi/vCenter server, then have to select, Datacenter, then Host and finally the Virtual Machine as shown in Figure 6.8. This virtual machine that from it will extract information for a forensic purpose.

Figure 6.8: Choose Virtual Machine_1 from Available Virtual Machines.
3. **Access Virtual Machine Forensic Page:** After the user selected the virtual machine, the user has to press **GetForensicData** button in home page to access VM’s forensic page where a window with a welcome message to the selected Virtual Machine appears as shown in Figure 6.9. Then the forensic page for the selected virtual machine appears as shown in Figure 6.10. Details of virtual machine forensics page features will describe below.

![Figure 6.9: Welcome Message when accessing The Virtual Machine Forensics Page.](image1)

![Figure 6.10: Virtual Machine Forensic Page.](image2)
- **Extract Storage System Information of Host**: When the user pressed this button a text file is downloaded that contains information about storage system of the selected host as shown in Figure 6.11. This information command “esxcfg-info-s” in ESXi-utilities that used to map storage volumes to a physical device and related information observed device names that bear the model and a serial number of hard disks connected to ESXi, and this would be important for the investigation that requires the seizure of physical evidence or contraband from a physical device.

![Extract Storage System Information](image)

*Figure 6.11: Extract Storage System Information.*

- **Create Virtual Machine Snapshot (Live Forensic)**: When the user pressed this button a window required file name for new Snapshot and after writing Snapshot name and click ok a message appeared to confirm the creation of the snapshot as shown in Figure 6.12. The Virtual machine snapshot is a state of the virtual machine, at a specific point in time such as a restore point in windows. Snapshots are helpful in restoring data locally in the event of data in case of loss or corruption. This snapshot lets you automate the capture of numerous pieces of volatile information that are critical during forensic investigation process and incident response. This information including Open files, Users on a system, network status and connections, TCP and UDP port information, Running
processes and applications. A feature of VM snapshot for the selected virtual machines can be as useful for the forensic purpose as live forensic through reconstructing timeline about previous activities occurred on the virtual machine.

- **Show All Virtual Machine Files**: When the user pressed on **Show All Virtual Machine Files** button, a text file is a download that contains information about the selected virtual machine files as shown in Figure 6.13.

**Figure 6.12**: Create Snapshot of Selected Virtual Machine.

**Figure 6.13**: Extract and List Selected Virtual Machine Files.
- **Show All Virtual Machine Disk Files**: When the user pressed on **Show All Virtual Machine Disk Files** button, a text file is downloaded that contains information about the selected virtual machine Disk files as shown in Figure 6.14.

![Figure 6.14](image)

**Figure 6.14**: Extract and List Selected Virtual Machine Disk Files.

- **Show VM Log Files**: When the user pressed on **Show VM Log Files** button, a text file is downloaded that contains information about the selected virtual machine Log files as shown in Figure 6.15.

![Figure 6.15](image)

**Figure 6.15**: Extract and List Selected Virtual Machine Log Files.

- **Show VM Nvram Files**: When the user pressed **Show VM Nvram Files** button, a text file is downloaded that contains information about the selected virtual machine Nvram files as shown in Figure 6.16.
Figure 6.16: Extract and List Selected Virtual Machine Nvram Files.

- **Power On, Power Off and Suspend Virtual Machine:** The proposed system provides an option to control the status of the select virtual machines such as turn on, turn off and suspend.

- **Acquire OVF file (Dead Forensics):** When the user pressed Acquire OVF file (Dead Forensics) button, an OVF file with a text file are downloaded. This text file contains information about the Acquired Open Virtualization Format (OVF) file information such as start time, end time and total and hash values of exported OFV file as shown in Figure 6.17. The acquired OVF file is an encrypted and compressed file so that there is a need to decompress this file to be suitable to the forensic analysis process using forensic tools like FTK Imager. We used a free VBoxManger.exe that comes with VirtualBox. This is a command line tool located under C:\Program Files\Oracle\VirtualBox. This tool gives you the option to convert the compressed vmdk (or a regular vmkd) into several formats: VHD, VDI, VMDK, and Raw. After the conversion, the decompressed file is in a format that can work with like any other normal VMDK file.

  The syntax is: “VboxManage.exe clonehd "Source Path of compressed VMDK file" "destination Path to store decompressed VMDK file" --format VMDK “

  Once the OVF file is decompressed as shown in Figure 6.18, then create an image and its integrity verified, the image ready to be analyzed by using forensic analysis tools such as Encase, Access Data Forensic Toolkit (FTK), and The Sleuth Kit (TSK).
6.4.6 System Evaluation

In order to properly evaluate the performance and capabilities of the proposed HFAA application, two test scenarios were created. Each scenario highlights a specific feature or capability to show the HFAA application can be used to conduct digital forensic image acquisitions in an actually virtualized environment. Data integrity is very significant in digital forensics to ensure that digital evince can be accepted as admissible evidence in the court of law. And the performance of proposed system also very important for providing rapid forensic tool especially with massive data. Therefore, we suggest two scenarios to evaluate the proposed system based on image integrity and system performance as follows:

- **Scenario 1:** Image integrity is of the most important when conducting a digital forensics investigation. Once an image of the target hard drive or file is created, a forensics investigator must ensure the integrity of the image remains true to the original. Failure to ensure image integrity could result in false data being retrieved or digital evidence not being admissible in court. This scenario highlights the ability of the HFAA application to ensure image integrity through each step of the image acquisition process. HFAA tracks the integrity of the image and if the integrity is compromised, the program can detect this change and notify the user accordingly. In above scenario 1, the image
integrity verification function was tested in the process of exported OVF file through generating sha1 and MD5 hash values as shown in Figure 6.17 that can use after that in the verification process.

- **Scenario 2:** Various virtual machines and files of all different sizes can exist on an ESXi server. The size of a file to be acquired can have an impact on the amount of time it takes to acquire that file. The time required to acquire and export of varying sizes of OVF file from different virtual machines will be examined in this scenario. This scenario looks at how the exporting process involves the duration of time it requires to take on different size of OVF files. This scenario is split down into three parts to export three OVF files of three virtual machines that stored in one of the two ESXi servers in the experimental environment. The exporting process performed by the HFAA is compared with the exporting process using VMware vSphere client program. This comparison is shown in Table 6.2 and Figure 6.19. From this scenario, noticed that the proposed system-HFAA is faster than the vSphere client program in exporting OVF files. Therefore, the proposed system can take less time in exporting and acquiring virtual machine files from ESXi servers. This means it saves acquisition time and the entire forensic process as well as develop new fast forensics tools in the future.

### Table 6.2: Comparison between VMware vSphere Client and HFAA for Exportation of OVF File.

<table>
<thead>
<tr>
<th>Virtual Machines</th>
<th>OVF File Size</th>
<th>VMware vSphere Client</th>
<th>HFAA (Proposed System)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Start Time</td>
<td>Completed Time</td>
<td>Duration in Minutes</td>
</tr>
<tr>
<td></td>
<td>Start Time</td>
<td>Completed Time</td>
<td>Duration in Minutes</td>
</tr>
<tr>
<td>Virtual Machine 1</td>
<td>914 MB</td>
<td>10:32:15 PM</td>
<td>10:37:51 PM</td>
</tr>
</tbody>
</table>
Figure 6.19: Comparison between VMware vSphere Client and HFAA.

6.4.7 System Limitations

There are a number of limitations that exist in the current version of the proposed HFAA application. These limitations are solvable and require additional development time that will be in future versions. Some of these limitations are:

- Virtual machine contains several types of files, as shown above. Currently, HFAA can export only OVF file that contains VMDK files of the virtual machine but not all virtual machine files.
- The application does not check first to see if there is enough space available before exporting the OVF file.
- HFAA does not check the state of the virtual machine before the acquisition process.
- HFAA must utilize root user credentials in order to properly function and the tool executes. This indicates there is a possibility that HFAA could compromise the stability or security of an ESXi/vCenter server. Although unlikely, the tool could malfunction and cause an errant command to be executed on the ESXi server, which could harm or damage the ESXi/vCenter server and the virtual machines running on it.
- HFAA doesn’t be checked to extract and acquire virtual machines stored on a remote storage device via different protocols such as fiber channel, Internet Small Computer System Interface (iSCSI), or Network File System (NFS) where the VMware ESXi
servers that may utilize a Storage Area Network (SAN) or Network Attached Storage (NAS) device.

- Extend the proposed application to work as Web or Mobile application as shown in Figure 6.20.

![Figure 6.20: Future Development of Proposed Application.]

### 6.5 Chapter Summary

This chapter introduced the design and implementation of HFAA- a forensic acquisition application for clustered VMware ESXi hypervisors that used in virtualized environments. The design supports to scale in a dynamic cloud computing environment where distributed clusters of hypervisors that share virtual machines and storage for providing better and on-demand services. This application aims to be utilized for extracting digital evidence from clustered VMware ESXi hypervisors for assisting the digital investigators in performing the digital investigation process. This application is an initial step for the digital investigators, practitioners, and researchers to develop new approaches and methods for evidence acquisition and extracting from clustered VMware ESXi hypervisors and hosted virtual machines in a forensically sound and timely fashion.