Server Virtualization Acquisition Using Live Forensics Method

Soni
Informatics Engineering
Universitas Muhammadiyah Riau
Pekanbaru, Indonesia
soni@umri.ac.id

Yudi Prayudi
Informatics Engineering
Universitas Islam Indonesia
Yogyakarta, Indonesia
prayudi@staff.uii.ac.id

Bambang Sugiantoro
Informatics Engineering
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
bambang.sugiantoro@uin-suka.ac.id

Didik Sudyana
Informatics Engineering
STMIK AMIK Riau
Pekanbaru, Indonesia
didik.sudyana@stmik-amik-riau.ac.id

Harun Mukhtar
Informatics Engineering
Universitas Muhammadiyah Riau
Pekanbaru, Indonesia
harunmukhtar@umri.ac.id

***Abstract*—Server virtualization is a technology that can run multiple operating systems simultaneously on one computer. The emergence of server virtualization invites a new crime gap that is different from the challenge of finding clues and digital evidence in uncovering cases of crime. This certainly makes it difficult for investigators to make acquisitions of one of the operating systems in server virtualization without disturbing and shutting down the computer given the importance of the server. So far, acquisition techniques are generally used singly which only contains one operating system. Therefore, it is necessary to have a technique to acquire server virtualization by using the live forensics method without interrupting or shutting down other running operating systems. The use of the live forensics method to acquire server virtualization is done by applying three acquisition techniques. Three acquisition technique models are carried out by acquiring one of the operating systems that are in the virtual machine on server virtualization through the Proxmox server without turning off the other operating systems that are running. Of the three acquisition models that have been tested, it is known that there are two models of acquisition techniques that are well used and recommended based on the situation and conditions that are occurring.**

Keywords—Digital forensics, Acquisition, Server Virtualization, Live Forensic

I. INTRODUCTION

Server virtualization is a technology that is currently growing rapidly. This is proven based on a survey report published by spiceworks.com, stating that 76% or more than three quarters of respondents use server virtualization in the data center. From these statistics, it appears that virtualization is most widely used and a few percent of respondents have also planned to use virtualization [1].

Virtualization can increase hardware usage by sharing and scheduling resources between multiple virtual machines on a single server so that the development of server virtualization can increase rapidly [2]. Based on news published by ictnext.net, it is confirmed that server virtualization has a positive impact on the company by offering efficiency in terms of investment requirements for purchasing physical servers to be less. With the lack of physical servers that must be stored in the data center, the need for floor space to place physical servers can be reduced [3].

Virtualization is a method for creating abstract computer resources from physical hardware devices to provide multiple virtual machines [4]. At present, virtualization plays a very important role in the world of information technology. This is proven by many companies that have used virtualization. In addition to saving the company's operational costs, virtualization also reduces the number of physical servers needed, namely by utilizing a physical hard disk space. Space can be divided into several parts that can later be used by virtual server machines. Thus the company does not need a lot of servers anymore because it can be accommodated and combined in 1 to 2 servers.

Such rapid development of virtualization will invite a new crime gap. [5] Crimes that occur by involving server virtualization have an impact on new challenges to find clues and uncover cases of crime that exist in server virtualization. If one virtual machine is used to commit a crime, of course it will make it difficult for investigators to acquire and analyze one of these virtual machines because it is impossible to make an acquisition of the entire server itself considering how much storage capacity of the entire server.

Computer acquisition is generally carried out singly where one computer only contains one operating system. But now one computer can load more than one operating system so that the right acquisition technique is needed to extract only the data that is open without taking all the data in the server computer. Unfortunately, there is no standard technique for acquiring server virtualization because there are several things that have different characteristics if one computer has many operating systems. Moreover, there is no research that discusses the acquisition of server virtualization. Existing research discusses analysis and acquisition on virtual machines from the client side such as virtual boxes and vmware. Therefore, it is necessary to do further research on how to acquire techniques in server virtualization [6].

In this study, it employed several techniques and ways to acquire server virtualization based on several literature reviews about the storage structure of server virtualization. Then from various kinds of acquisition techniques, the acquisition results were carried out for examination and analyzed to find out whether the acquisition results obtained could be read by forensic software. Furthermore, this study

also tried to figure out the file structure contained in server virtualization and whether it could recover the deleted file on one operating system on server virtualization. The results of the acquisition carried out from various types of acquisition could show which acquisition technique is the best and right as well as to be recommended for use in acquiring server virtualization.

Because the acquisition was carried out on server virtualization with the condition of the physical server still running, the acquisition used the live forensic method. Live forensics is a forensic method by gathering information, analyzing, and presenting it using various forensic tools when the system is still running [7].

II. RESEARCH REVIEW

The following discusses a review of the research that has been done previously relating to virtualization. The first research was conducted by [8] that studied sound forensics to obtain and analyze virtual servers on hard drives. The research also compares files that have been corrupted so that any files that have been added, deleted, edited and modified can be identified.

Subsequent research was conducted by [9] conducting experiments to understand the architecture and limitations of various VM at each stage of digital investigation analysis. The VM used in the study are: virtual box, vmware workstation, cooperative linux, and XEN desktops.

Another study conducted by [10] made a digital forensic investigation procedure and created a method for recovering damaged image files on the VMware workstation that aims to help investigators to carry out appropriate investigations and obtain data in accordance with the cases that occur.

Then [11] in his research conducted an analysis of the evidence of VMware workstation virtual machines using the forensic live view tool. The tool can protect VM evidence from data changes in the analysis process. The operating system used in virtual machines is the Windows XP operating system. In addition, Khangar et al discussed various challenges that occur when collecting evidence.

In addition to the above research, [12] also conducted research by looking for evidence of activities carried out by virtual machines that can be recovered or restored so that further investigation can be done. The virtual machine used in his research is a virtual box.

III. METHODOLOGY

In summary, the methods and stages of the research can be described as in Figure 1 below.

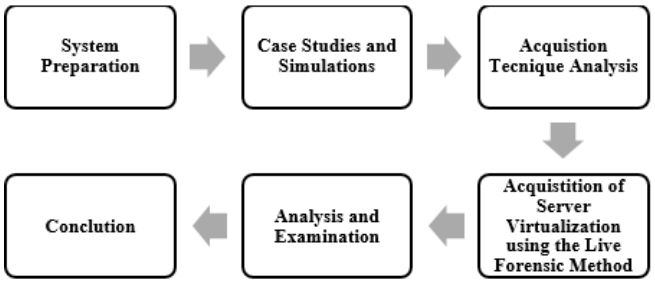

Figure 1 – Methodology

IV. RESULT AND DISCUSSION

A. *System Preparation*

Server virtualization was built into the physical server where the Linux proxmox virtual environment operating system was installed and in the Proxmox server there are two virtual machines. The two operating systems in the virtual machine are the Ubuntu Linux operating system and the Microsoft Windows 10 operating system. Table 1 below is a list of hardware and software specifications needed and used in building server virtualization.

Table 1. System Preparation

No	Hardware / Software	Description
1	PC Server, Processor AMD Athlon II Dual Core X2 270 3.4 Ghz, Hardisk 160 GB, RAM 4 GB	Hardware
2	PC Client, Processor AMD Athlon II Dual Core X2 270 3.4 Ghz, Hardisk 160 GB, RAM 2 GB	Hardware
3	Proxmox Virtual Environment 4.3 operational system	Server
4	Linux Ubuntu Desktop 16.04	System Operation
5	Microsoft Windows 10	System Operation
6	Belkasoft Evidence Center	Forensic Tools
7	The Sleuth Kit Autopsy 4.1.1	Forensic Tools

Then the physical server would be installed with a special operating system for server virtualization, proxmox. Then two Ubuntu Linux and Windows 10 operating systems were implemented. Both operating systems run in the virtual machine on Proxmox server virtualization.

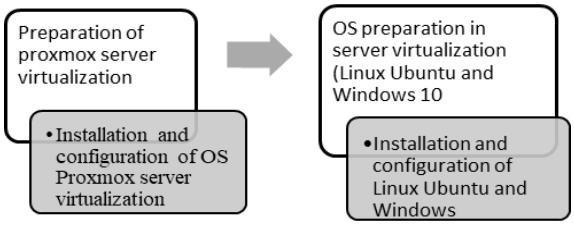

Figure 2 – System Preparation

In all of these scenarios, Digital Evidence First Responder (DEFR) needs to make a copy of digital evidence that is suspected to contain the necessary evidence. The acquisition procedures listed in SNI 27037: 2014 are as follows [13]

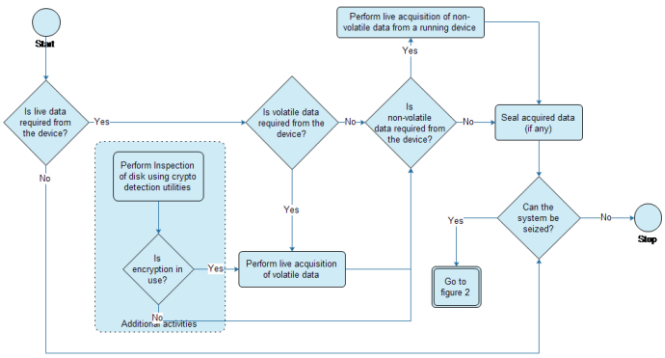

Figure 3 – SNI Acquisition 27037:2014

B. Case Study and Simulation

It is the stage of making a case simulation on server virtualization by installing a web server and deleting six files. Then it will be acquired and examined and analyze whether the web server and the six files can be recovered.

```
root@ubuntu:/home/ubuntu/Documents# md5sum *
c212fd1f1420a4b3cc651f731401397a  DAFTAR NAMA PELANGGAN MURCEAJA TAHUN 2016.xlsx
3cb48b95590100631c722acfa3cde99d  DATA.zip
3c046263432ef7a1d693eed36fb86df9  DCIM_01.jpg
d3aac2bcb523681971cedb19adac00c7  FILE WORD.docx
78edb70e224ae5a2cea90569e028a6ca  GANJA.jpg
1cc4d30cfa91d8996a0f78168e58182e  SABU.png
root@ubuntu:/home/ubuntu/Documents#
```

Figure 4 – Case Studies and Simulations

Figure 3 shows the six files that will be deleted from the vm operating system for Ubuntu. The six files consist of 1 .xlsx file, 1 file.zip, 2 file.jpg, 1.docx file and 1 file.png. The six files in Figure 4.2 also have md5 hash value each. Next, make six files stored in the folder/home/ubuntu/Document/with Shift+Delete, which is permanently deleting files so they are not stored in the trash folder.

C. Acquisition Technical Analysis

1. Analysis of Acquisition Technique of Model I
   Logical Volume Manager (LVM) is a virtual hard disk storage that is used to simplify the disk management process from a large hard drive. In addition, the users can also add/delete/change the size of the Logical Volume Manager (LVM) that has been created [14].

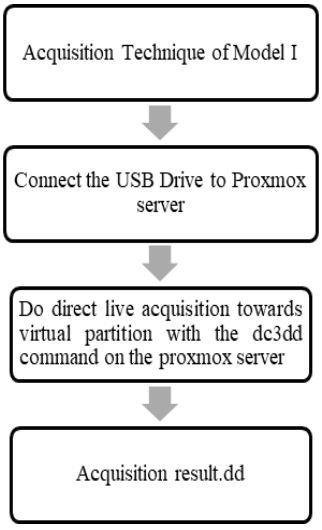

Figure 5 – Analysis of Acquisition Technique of Model I

2. Analysis of Acquisition Technique of Model II
   Proxmox provides a backup feature. The backup feature serves to back up the entire file system contents to the operating system that is still running, the partition and the data contained in the proxmox vm server. The backup results are .vma connectivity and have been compressed so that they only have a size of one third of the total file system in the partition [13].

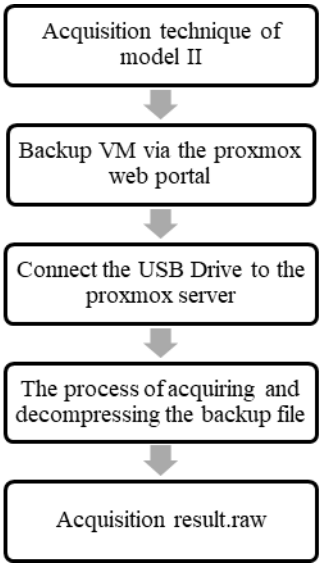

Figure 6 – Analysis of Acquisition Technique of Model II

3. Analysis of Acquisition Technique of Model III
   Proxmox provides a feature to connect the usb drive to the guest os so that based on an explanation of existing theoretical analysis it will be used to apply the acquisition of model III virtualization techniques.

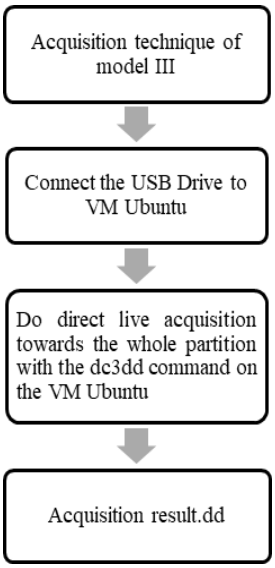

Figure 7 – Analysis of Acquisition Technique of Model III

D. Acquisition of Server Virtualization using the Live Forensic Method

The figure below explains the techniques used in acquiring server virtualization using 3 acquisition techniques

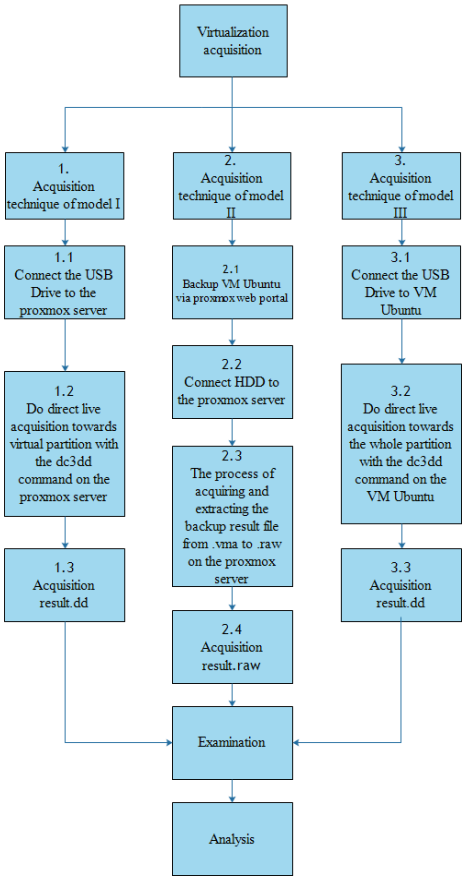

Figure 8 – Acquisition of Server Virtualization

Model I Acquisition Technique is a technique that is carried out by directly acquiring an Ubuntu virtual partition through the Proxmox server. Then the model II acquisition technique is an acquisition technique that is carried out by first making a backup of the ubuntu VM, the backup results are extension .vma. Then the backup.vma file is extracted so that the extension changes to .raw. While the model III acquisition technique is an acquisition technique that is carried out by acquiring directly the hard drive partition on the ubuntu VM. Furthermore, the acquisition results will be copied to the USB drive. Because the Ubuntu OS is in the Proxmox virtual server, so it must first configure 100.conf so that the USB drive can be read by the Ubuntu OS. Then the three results of the acquisition will be examined and analyzed to find out which acquisition technique is the right and the best and is recommended to be used to acquire server virtualization.

1. *Acquisition Technique of Server Virtualization Model I*

Model I acquisition technique is an acquisition technique that is carried out by conducting live acquisition directly on the proxmox server to one of the virtual servers inside using the dc3dd command. In proxmox, the virtual operating system partition is stored in local-lvm at /dev/mapper/. In /dev/mapper there are 2 OS namely pve-vm-100- -disk- -1 and pve-vm-102- -disk- -1. Because only the Ubuntu OS will be acquired which is located on vm - -100, the acquisition will only be a mapper file on pve-vm-100- -disk- -1. The results of model I acquisition techniques can be seen in Figure 9 below:

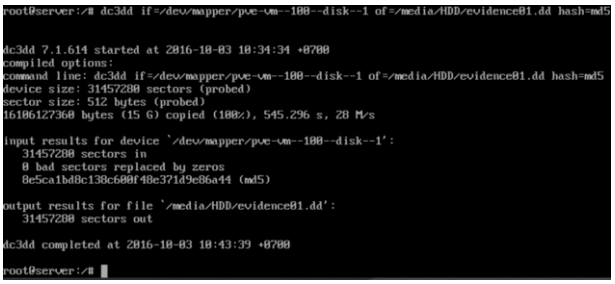

Figure 9 – Imaging Result of Acquisition Technique Method I

Figure 9 illustrates the process carried out in acquiring server virtualization using the dc3dd command. In the picture, it is explained that the acquired virtual partition is in pve-vm-100 - disk-1. The acquisition was carried out on 03-10-2010 at 10:34:34 and finished at 10:43:49.

2. *Acquisition Technique of Server Virtualization Model II*

The model II acquisition technique is the acquisition process that is done by backuping the virtual vm first which can be backed up by using the proxmox web portal by accessing the ip address and TCP port 8006, namely: https://192.168.0.44:8006 and will generate the zvdump-qemu-100-2016_10_03-10_47_04.vma file. The process and results of the acquisition of model II will be illustrated in the following picture 4.8:

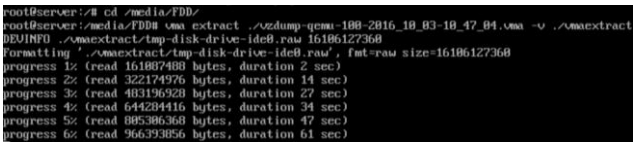

Figure 10 – Imaging Result of Acquisition Technique Method II

Figure 10 shows the extraction process from zvdump-qemu-100-2016_10_03-10_47_04.vma to disk-drive-ide0.raw. This process needs to be carried out so that the acquisition results can be read by forensic tools for examination and analysis.

3. *Acquisition Technique of Server Virtualization Model III*

The model III acquisition technique is a live acquisition technique that is carried out by acquiring a whole partition on the ubuntu VM server that is on the Proxmox virtual server using the dc3dd command by connecting the usb to the ubuntu virtual server and passing several procedures and stages to be able to connect to the ubuntu vm. The process and results of the acquisition in model III will be drawn in the following figure:

Figure 11 – Imaging Result of Acquisition Technique Method III

Figure 11 is a process that is carried out in acquiring the entire contents of partitions in the ubuntu operating system running in a virtual machine. The acquisition process started at 11:31:09 and finished at 11:52:28. The result of model III acquisition has a hash value of md5 995D2BFB623C5640B570270E7F953CBC.

E. Examination and Analysis Using Autopsy

After successfully making acquisitions with three models I, II and III, the next is conducting an examination and analyzing the results of the acquisition with a forensic tool the sleut with autopsy. The results obtained from the autopsy, namely the overall results of the acquisition can be read all by the autopsy of the acquisition techniques of model I, model II and model III. The results of the examination using the autopsy tool can be seen in the following figure 4.10:

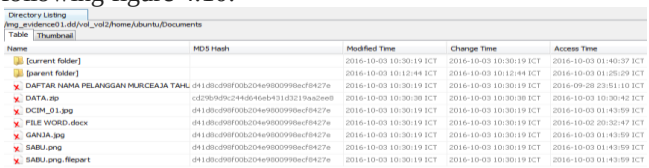

Figure 12 – Result of Autopsy Examination and Analysis

Figure 12 above shows that the results of the acquisition carried out can find deleted files in case simulations. But the hash value of md5 from the six files has changed. The results of the examination carried out also succeeded in reading all the system files contained in ubuntu OS which can be seen in Figure 12 below:

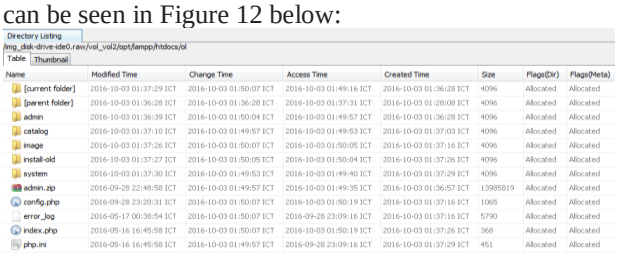

Figure 13 – Directory in autopsy

Figure 13 shows the location of the stored web server folder in /opt/lampp/htdocs/ol. The directory consists of 5 folders, 1 zip and 5 other files.

F. Examination and Analysis Using Belkasoft

After the acquisition was carried out successfully, the next stage is to extract and analyze the data on the results of the acquisition of models I, II and III which are conducted using the Belkasoft Evidence Center. From the results of the examination carried out, it turns out that the three acquisition models can read the entire contents of the file in a partition within the ubuntu VM. Furthermore, it can rediscover the six files that have been deleted based on simulated cases that have been scanned. It can be shown in Figure 14 below:

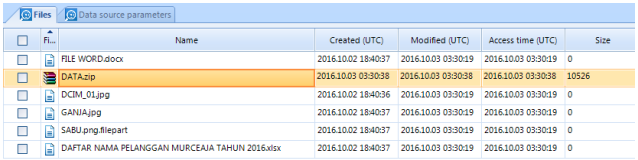

Figure 14 – Result of Belkasoft Examination and Analysis

Figure 14 shows six files found successfully using the belkasoft tool. But the size and md5 of the six files have changed to 0 byte and do not match the original data.

From the extraction results, it also found one Microsoft Excel file with the name 1808.xlsx and one Microsoft Word file with the name 1809.docx. Then the md5 hash values of the two files are checked. It turns out that both files have the same hash value and also if opened the file contains the same data as the file on the data before being deleted. The two files are shown in Figure 15 below:

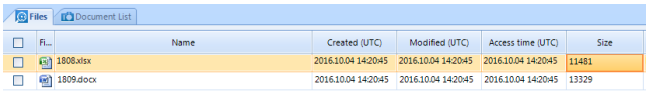

Figure 15 – Office File Discovery Directory

From the results of data extraction using Belkasoft, it also found the storage location of the web server and web server files can be read with the Belkasoft Evidence Center tool. The storage location file from the web server can be seen in Figure 16.

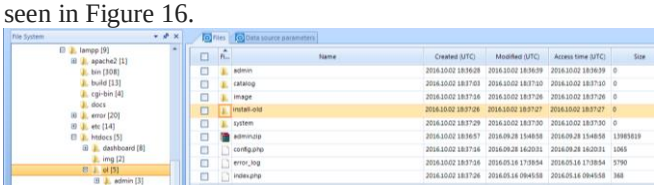

Figure 16 – Directory in Belkasfot

The acquisition results that have been carried out on server virtualization using models I, II, and III were declared successful because the vm partition on the proxmox server was successfully acquired and all files contained in the partition can be read by forensic software, belkasoft and autopsy. Moreover, the deleted file can be rediscovered. However, the file cannot be recovered because the size and md5 of the file has changed and is not in accordance with the original data. This is proven by matching the hash value of the recovery file with the file hash value before being deleted.

During the acquisition process, the three acquisition model techniques to produce analysis can be summarized in table 2 below:

Table 2 – Comparison Table of 3 Acquisition Techniques of Server Virtualization

No	Indicator	Acquisition Model I	Acquisition Model II	Acquisition Model III
1	The method used in acquiring server virtualization	Acquire the drive stored in the lvm server proxmox partition	Acquire by utilizing the backup feature through the proxmox web portal	Acquire the entire file system directly through ubuntu operating system
2	Hash value generated	Produce the same hash value as Acquisition Model II	Produce the same hash value as Acquisition Model I	Produce different hash value from Acquisition Model I & II
3	Acquisition Result	Can be read by Tools Forensic	Can be read by Tools Forensic	Can be read by Tools Forensic
4	Rediscover deleted files	Yes	Yes	Yes
5	Forensic Approach	In accordance with	In accordance with	Less in accordance with

No	Indicator	Acquisition Model I	Acquisition Model II	Acquisition Model III
		Acquisition Procedure of SNI 27037:2014	Acquisition Procedure of SNI 27037:2014	Acquisition Procedure of SNI 27037:2014
6	Stages carried out during the acquisition	2 stages	3 stages	2 stages
7	Use of time	00:11:15	00:20:40	00:28:23
8	There is a backup feature	-	There is	-

In table 2 above there are eight indicators. Each indicator in each acquisition model has the same process and there are also different processes. Each of these indicators will be explained in the following points:

Table 3. Use of time in each acquisition model

No	Stage of Acquisition	Acquisition Model I	Acquisition Model II	Acquisition Model III
1	Connect the usb drive to Proxmox server	00:02:10	00:02:07	-
2	Connect the usb drive to VM Ubuntu	-	-	00:07:03
3	Acquisition process	00:09:05	00:11:16	00:21:20
4	Backup VM via portal web proxmox	-	00:08:17	-

Table 3 above illustrates the time usage in each acquisition model. In model I the time used only takes 11 minutes 15 seconds with two main stages. Then in model II it takes 20 minutes 40 seconds through three stages. Whereas in model III, it takes 28 minutes 23 seconds with two stages being passed.

Based on the indicators outlined in table 2 and based on the trials that have been carried out, there are two acquisition techniques that can be recommended for use in acquiring server virtualization, both of which are model I and II acquisition techniques. Each acquisition model is better and recommended based on existing situations and conditions. In terms of time usage, model I acquisition techniques are better because they use the least amount of time compared to the other two acquisition techniques. Model I acquisition techniques can be used under conditions when the virtualization of the server used is private property. While the model II acquisition technique is recommended if the server to be acquired uses another server service provider as its data center and the location of the data center is also located in a remote location. In this condition, the acquisition technique of model II is a better acquisition technique and is recommended because the acquisition can be done through the proxmox web portal using the backup feature. Therefore, when making an acquisition, the investigator does not need to come directly to the server service provider.

V. CONCLUSION

Based on the stages and results of the analysis of the three techniques of the acquisition model, it is known that there are two acquisition techniques that are recommended and used in acquiring server virtualization. The two techniques have their respective advantages and are judged to be better according to the situation and conditions that occur. Both acquisition techniques are model I and II acquisition techniques. Model I acquisition is better used when viewed from the side of time, because the time used is the least compared to the other two acquisition techniques, and model I acquisition techniques are good to use if server virtualization is used alone. Whereas model II acquisition technique is recommended and is good to use if server virtualization uses server provider services as its data center and its location is far away because the acquisition process can be done using backups through the proxmox web portal. It means that investigators do not need to come directly to the location of the server provider.

REFERENCES

[1] Spiceworks.com, “State of it report,” 2016. [Online]. Available: http://www.spiceworks.com/marketing/state-of-it/report/. [Accessed: 19-Jun-2016].

[2] S. Zahedi, “Degree project Virtualization Security Threat Forensic and Environment Safeguarding,” 2014.

[3] Ictnext.net, “Survei 60 enterprise di asean perluas virtualisasi server hingga 2014,” 2014. .

[4] D. Shackleford, *Virtualization Security: Protecting Virtualized Environments*. Canada: Wiley Publishing, 2012.

[5] D. Sudyana, R. T. Putra, and S. Soni, “Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037 : 2014,” Sink. - J. Publ. Informatics Eng. Res., vol. 3, no. 2, 2019.

[6] Soni, Y. Prayudi, and B. Sugiantoro, “Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic,” Teknomatika, vol. 9, no. 2, 2017.

[7] M. Rafique and M. N. A. Khan, “Exploring Static and Live Digital Forensics: Methods, Practices and Tools,” *Int. J. Sci. Eng. Res.*, vol. 4, no. 10, pp. 1048–1056, 2013.

[8] M. Hirwani, P. Y. Pan, P. D. Johnson, P. B. Stackpole, and B. T. G. College, “Forensic Analysis of VMware Hard Disks,” 2011.

[9] F. M. Patterson, “The Implications of Virtual Environments In Digital Forensic Investigations,” *J. Chem. Inf. Model.*, vol. 53, pp. 1689–1699, 2011.

[10] S. Lim, B. Yoo, J. Park, K. Byun, and S. Lee, “A research on the investigation method of digital forensics for a VMware Workstation’s virtual machine,” *Math. Comput. Model.*, vol. 55, no. 1–2, pp. 151–160, 2012.

[11] S. Khangar, G. Nagpur, and R. Dharaskar, “Digital Forensic Investigation for Virtual Machines,” *Ijmo.Org*, vol. 2, no. 6, pp. 663–666, 2012.

[12] C. Neal, “Forensic Recovery of Evidence From Deleted Oracle Virtualbox Virtual Machines,” no. December, 2013.

[13] Badan Standarisasi Nasional, *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta, 2014.

[14] S. M. Cheng, *Proxmox High Availability*. 2014.