**Scientific Journal of Informatics**
Vol. 6, No. 1, May 2019
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

# Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method

**Didik Sudyana [1], Nora Lizarti [2]**

[1] Department of Informatics Engineering,
STMIK Amik Riau
[2] Department of Informatics Engineering,
STMIK Amik Riau
Email: [1]didik.sudyana@stmik-amik-riau.ac.id , [2]nora.lizarti@stmik-amik-riau.ac.id

**Abstract**

The high rate of development of IAAS Cloud Computing model on server virtualization is in line with the high number of cyber crimes, and when it occurs, a digital forensic investigation is needed. However, it raises issues related to the acquisition of digital evidence. In general, the acquisition model is done only to one operating system, while in virtualization there is more than one, so the general method cannot be used on it because it takes only for single operating system and cannot acquire the whole data server related privacy data in other virtual operating systems. So, in this research will make the acquisition system of server virtualization Proxmox using the live forensic method and it can acquire virtual operating system without disrupting the overall data server and by the principle of digital forensics. From the experiment results, it can be seen that the system can acquire the selected operating system. Then the whole data operating system can be examined by forensic tools, and the deleted data can be recovered. The acquisition system can be a reference for investigators to investigate the IAAS Cloud Computing model on Proxmox virtualization and this system is easy to use.

**Keywords**: Cloud Computing, Cloud Forensics, Virtualization Forensics

## 1. INTRODUCTION

Cloud Computing is a technological development that is quite warmly discussed in recent years. Cloud Computing enables Internet-connected users to share their resources such as files, applications, services with others who are also connected to the Internet quickly and efficiently [1]. There are three types of Cloud Computing models currently available, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Services (SaaS). From the three types of models, the IAAS model is currently the highest growth and usage model where there is an increase of up to 36.8% in 2017 [2].

Virtualization is one of the models of IAAS, and it provides virtual storage and computing services to users that are only possible through virtualization [3]. Many virtualization products are currently in this world. Among them are Amazon, OpenStack, VMware ESXi, Microsoft Hyper-V, and Proxmox.

The high rate of Cloud growth in IAAS is in line with the high level of cybercrime that occurs in IAAS services [4]. Cybercrime is a violation of law that uses computer technology based on the sophistication of the development of internet technology [5]. When a cybercrime in Cloud Computing takes place, it used a process with a scientific method known as digital forensics to reveal evidence of its crime [6].

One of the primary important from digital forensics is the acquisition. The acquisition is a process for making copies of digital evidence and documenting the methodology used, and the activities are undertaken [7]. The acquiring officer must select the most appropriate method based on the situation, cost and time, and document the selected decision to use specific methods and appropriate tools. The acquisition process becomes essential because if there is a mistake in the acquisition process, then the digital evidence obtained will not be used and certainly will not be a guide in the disclosure of cases involving this technology.

The acquisition is usually made on a computer with one operating system, but if there is a crime on server virtualization and then acquisition, there is no general acquisition procedure. Because in virtualization, one physical server loads multiple operating systems so that if a general computer acquisition procedure is performed, then the entire operating system in virtualization will come along. This technique will undoubtedly waste much time because to acquire all physical server data takes a very long time and violates the privacy associated with innocent others' data in other virtual operating systems.

Each virtualization has a different file and disk structure. So the acquisition techniques virtualized on Amazon products will be different from those on Proxmox. There are already several researchers who conduct research related to the acquisition process of the IAAS, including research conducted by [8] where they explore the acquisition techniques and evaluate tools against Amazon EC2 which is a server virtualization service provider. Then [9] did digital forensic investigation research on the IAAS Cloud Stack environment. Whereas [10] did the study about the acquisition of digital evidence metadata against OpenStack. The next is research by [11] who investigate VMWare Workstation by creating a recovery method for the damaged virtual OS which it can assist investigators in finding digital evidence. The last is research was completed by [12] who made an analysis of VirtualBox virtualization and performed procedures for recovering deleted virtual machines using FTK and autopsy tools. So on this research will focus on how to make the digital acquisition system on Proxmox virtualization because each virtualization has different file and disk structure.

Because the acquisition that will be done against of server virtualization with the physical server condition is still running, so the acquisition will use Live Forensic method. As mentioned by [13] that Live Forensics is a forensic method by gathering information, analyzing, and presenting it using various forensic tools while the system is still running.

The Live Forensic method used in the acquisition system uses the guidance of SNI 27037: 2014 in the Live Acquisition section. The system that was built later will run portable and does not require the installation of an acquisition system on Proxmox to reduce intervention in evidence. The system only needs to be copied into the Proxmox Server and executed immediately.

This system will have several menu options such as menus for mounting USB, menus to see a list of existing virtual operating systems, and a core menu, namely the acquisition menu. In the acquisition menu, there will be an option to choose the operating system to be acquired. This menu is a solution to the problem mentioned earlier that the acquisition procedure is carried out only for the desired operating system and not the entire contents of the Proxmox server hard drive.

After the selection of the operating system to be acquired, the system will start working to conduct live forensic acquisition procedures. The acquisition data is stored on external drives and at the same time preservation of evidence is carried out by calculating the hash code on the evidence of the acquisition. Therefore, it is hoped that this research can help to conduct forensic investigations of IAAS Cloud Computing in Proxmox.

## 2. METHODS

In this study, the acquisition method was carried out using the Live Forensics method of non-volatile data based on guidelines in the Indonesian National Standard (SNI) 27037: 2014 [7]. The method can be seen in Figure 1 below.

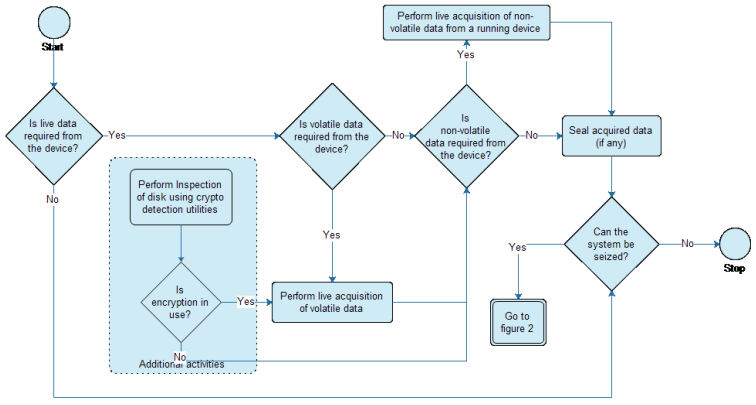


Figure 1. Acquisition Method on SNI 27037:2014

In the SNI 27037: 2014, it is explained that the steps to be taken for the acquisition process, namely the first is to determine the type of acquisition used, determine the type of data acquired, conduct the acquisition procedure, perform the seal acquired data procedure for the hashing process with MD5 then verifying the authenticity of the acquisition file .

Regarding the acquisition procedure carried out only on the system needed, this can be done because it has been regulated in the acquisition procedure in SNI

27037: 2014 called Partial Acquisition. It is stated that a partial acquisition is an acquisition made on a chosen system or chosen data only. The requirements for partial acquisition are as follows:

a. Storage capacity is too large for acquisition
b. The importance of the system so that it is not possible to turn off the system
c. When the data acquired is only part of the data needed
d. When limited by law enforcement such as search warrants that limit the scope of the acquisition

The four requirements are fulfilled in this study. So that a partial acquisition procedure can be carried out. When a decision has been made to make a partial acquisition, the activities for the acquisition include the following:

a. Identify folders, files or any other relevant data to obtain the desired data
b. Partial acquisition of the data for further identification.

The research methodology that will be carried out to complete this research are as follows:

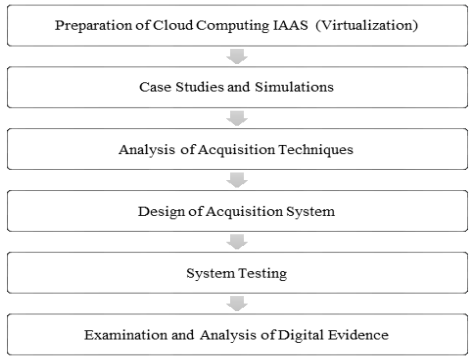


Figure 2. The research methodology

### 2.1. IAAS Cloud Computing System Preparation (Virtualization)

It is a step in preparing the hardware and software specifications used in the research is to design and implement server virtualization, such as installing and configuring Proxmox server system, making two virtual machines Microsoft Windows 10 and one virtual machine Linux Ubuntu.

### 2.2. Case Studies and Simulations

It is a step to create a case simulation on Cloud Computing IAAS server virtualization by creating a simulation wherein Virtual Windows 10 will be tried to delete some files. Before deleting, first is done hash code calculation for each file to be deleted to ensure that the file will be recovered after the acquisition process is a properly deleted file in the beginning. The purpose of recovery on deleted files is to find out whether the action to delete files in virtualization can be recovered.

### 2.3. Analysis of Acquisition Techniques

It is a step to analyze the theory about acquisition technique and theory about virtualization storage. Then from the analysis results, it will be used to make the acquisition of Cloud Computing IAAS on the Proxmox server virtualization. At this stage, the acquisition will be carried out within Proxmox on one Microsoft Windows 10.

### 2.4. Design of Acquisition System

In this stage, it will be built an application system for acquisition based on technical analysis that has been done previously. The acquisition system is built using the Bash Shell programming language. The reason for using this language because the acquisition system will be used on Linux-based text operating system.

### 2.5. System Testing

After the system is designed, it will be tested on whether the system successfully makes one acquisition of the virtual operating system on Proxmox. Testing is also done to see if the system succeeded in calculating hash code from digital evidence of acquisition result.

### 2.6. Examination and Analysis of Digital Evidence

This stage will do by extraction of digital evidence. Digital evidence that can be expressed as valid evidence is the evidence which can read the file structure and folder by forensic analysis software. After this stage completes, the next is to analyze digital evidence.

The analysis will be done by thoroughly checking the structure of files and folders and then perform the recovery process of data that has been deleted previously.

## 3. RESULT AND DISCUSSION

### 3.1 Preparation System

This stage is involving some tasks, namely: to implement the server virtualization, to configure the Proxmox server, and to configure the virtual machine that is Linux Ubuntu and the operating system Microsoft Windows 10. The computer specifications used as Server Virtualization are:

Table 1. List of Server Computer Specifications

| No | Hardware / Software | Information |
|---|---|---|
| 1 | PC Server, Processor Intel Core i3-2100 CPU@3.10Ghz, Hard drive 500 GB, RAM 8 GB | Hardware |
| 2 | Analyze PC, Processor Intel Core i5, Hard drive 720 GB, RAM 8 GB | Hardware |
| 3 | Operating system Proxmox Virtual Environment 4.3 | Server |
| 4 | Linux Ubuntu Desktop 16.10 | Virtual machine |
| 5 | Microsoft Windows 10 | Virtual machine |
| 6 | The Sleuth Kit Autopsy 4.1.1 | Forensic Tools |

### 3.2 Case Studies and Simulations

In this stage, a case simulation on IAAS Cloud Computing server virtualization will be done by deleting some files and calculating the hash code for every file. Four files have been prepared to be deleted with various file extensions. The four files are placed in the E partition on the virtual operating system with Win10-Suspect code. The hash value of the four files can be seen in Table 2 below.

Table 2. List of The Hash Value

| No | File Name | File Size | MD5 Value |
|---|---|---|---|
| 1 | E:\EXCEL.xlsx | 11.21 KB | C212FD1F1420A4B3CC651F731401397A |
| 2 | E:\FOTO.jpg | 1.9 MB | 13B5D25108DF618AA7226A5B53DAEC41 |
| 3 | E:\PDF.pdf | 499.65 KB | D8D906BE73595C8E6CF080DF3D240B26 |
| 4 | E:\WORD.docx | 13.12 KB | 4CC5044834475523C5206A3D6994EF85 |

### 3.3 Analysis of Acquisition Techniques

This stage is to analyze the theory about Proxmox storage because the acquisition will involve the storage media used by Proxmox. So it takes supporting theories about how the storage media mechanism used by Proxmox.

According to [14] Proxmox uses LVM (Logical Volume Manager) technology to store data for all virtual operating system data. When the virtual operating system is created, it will be given one LVM partition for the operating system. One given LVM is assumed to be a hard drive used by a virtual operating system storing the entire data. So based on the explanation, it is concluded that to acquire Proxmox, it must do on the LVM partition based on the virtual operating system storage.

In Proxmox, after searching for the LVM partition, it was found that the entire LVM partition of the virtual operating system on Proxmox was in /dev/mapper. So the acquisition focuses on finding the virtual operating system that has the LVM partition which is in Proxmox, then do the acquisition process on the partition using dc3dd tools.

### 3.4 Design of Acquisition System

At the design stage of the system, it built an application system to make acquisitions based on technical analysis that has been done previously. The summary of the menu and submenu are:

1. Mounting USB
2. Acquisition of OS
    1) List OS
    2) Acquisition of OS
        a. Select a virtual OS
        b. Check the USB External mount status
        c. Check status dc3dd
        d.Acquisition process
        e.hashing md5
    3) Menu
    4) Get out
3. Umount USB

4. Exit

After the build system is completed, it is uploaded to the Proxmox server and placed in the /home/script/ folder to be executed and be tested. Figure 3 below is a preliminary view of the system menu that has been designed.

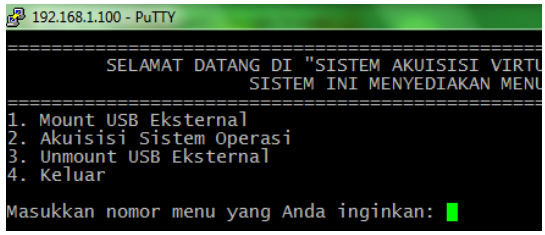


Figure 3. View system initial

To use the system, select the menu number and press enter. For example, if want to enter the "External USB Mount" menu, type the number 1 then enter, then the system will go to the menu Mount USB External.

### 3.5 System Testing

The first test procedure performed is to test the menu "Mount USB External". Figure 4 below is the test results of the USB External Mount menu when it runs successfully. USB External successfully detected in /dev/sdb1 and successfully mounted into folder /media/usb in Proxmox.

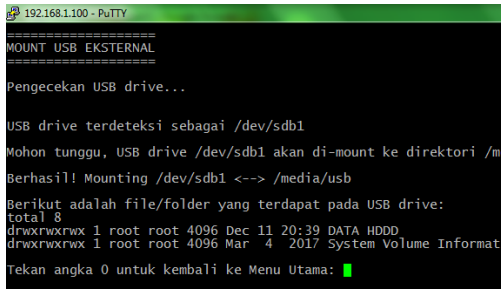


Figure 4. System Testing USB Mount Menu

The next test procedure is to test the Acquisition Operating System menu consisting of 4 sub menus. Figure 5 below is a display of Acquisition System menu and submenu display available.

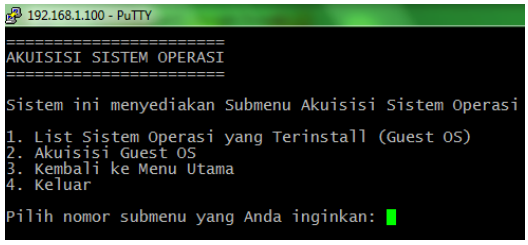


Figure 5. Display Menu Acquisition Operating System

The first sub-menu testing procedure is submenu "List Operating System" installed to see the list virtualization operating system. Figure 6 below is the result of testing the submenu. It successfully displays the list of installed operating systems in Proxmox server virtualization along with some information that is considered necessary such as Operating System status, Memory, and the capacity of the operating system Disk.

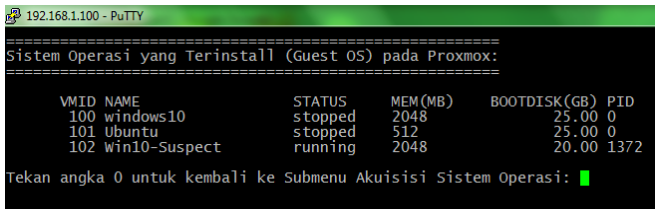


Figure 6. Testing Sub Menu "List Operating System"

The next testing procedure performed is on the Guest OS Acquisition submenu which is the core menu of this acquisition system. As planned, the virtual operating system that the acquisition test will attempt is the Win10-Suspect operating system with vmID 102.

After it, the system will start the acquisition process as designed previously. Before the acquisition process takes place, the system will perform the first three checking steps, that checking the External USB mount status, USB External free space status, and dc3dd status. Figure 7 is the result of checking status performed by the acquisition system before the acquisition process can be implemented.

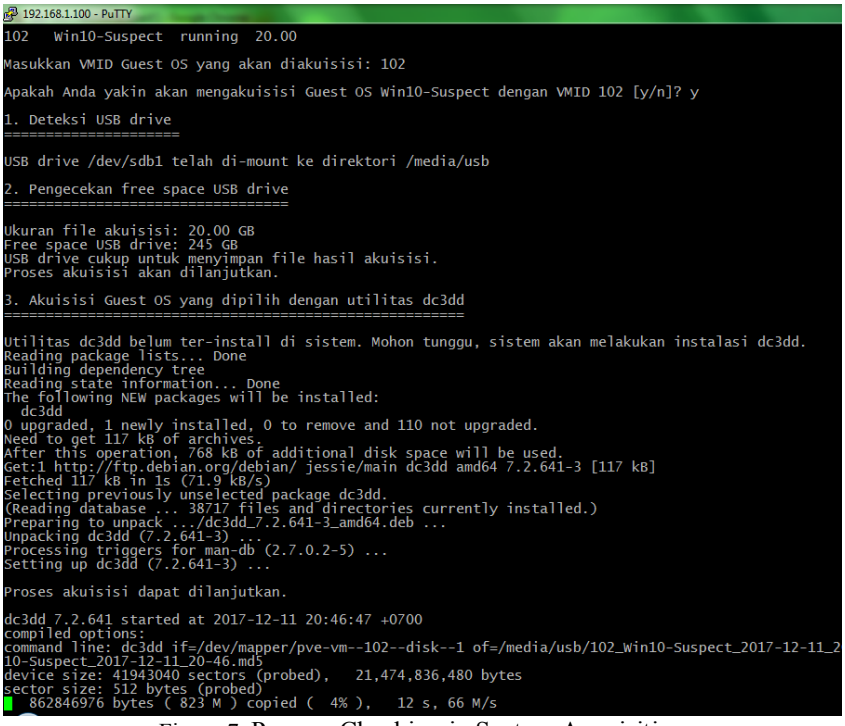


Figure 7. Process Checking in System Acquisition

After the checking procedure is complete, then the system will automatically continue the acquisition process. From Figure 7, after the checking process is complete, the acquisition process begins. The system also records the date and time of the commencement of the acquisition. In the tests that have been conducted, the acquisition process carried out on December 11, 2017, at 20:46:47. The acquired LVM is in /dev/mapper/pve-VM-102-disk-1, and by the system, the acquisition data will be placed in the directory /media/usb/ with the acquired file name 102_win10-Suspect_2017-12-11_20-46 .dd.

The acquisition process takes approximately 570 seconds and 30 seconds spent to perform the process of calculating the hash code of the acquisition file. So the total time spent to complete the acquisition process is 10 minutes. This process can be seen in Figure 8 below which is the result of completed acquisition testing carried out. Seen that the system provides a report on the acquisition process is completed on December 11, 2017, at 20:56:17 pm. There are 41943030 sectors by acquisition process, and the acquisition file has hash value md5 b83986f471da34dce1cdce812596ba0. The md5 hash value is also saved by the system into the /media/USB directory with filename 102_win10-Suspect_2017-12-11_20-45.md5.

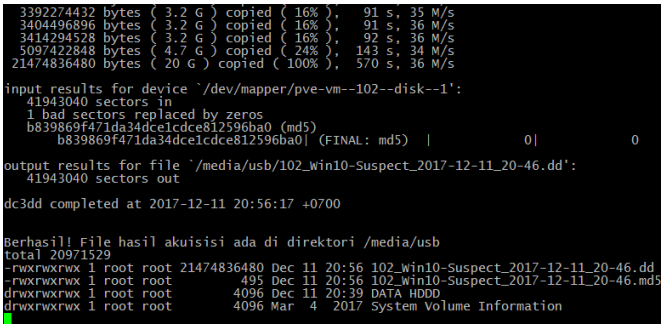


Figure 8. Results of testing the acquisition process

From all the results of testing the system performed, it can be seen that the acquisition system has been built successfully perform the acquisition of one of the virtual operating system planned.

### 3.6 Examination and Analysis of Evidence

Examination and analysis of evidence are conducted to examine the completed evidence acquired by extraction of digital evidence. This examination conducted using autopsy forensic software.

The evidence successfully extracted by autopsy and managed to read the whole structure of files and folders. Autopsy forensic software has detected three partitions which contain user data in the win10-Suspect virtual disk of the acquisition result. Figure 9 below is the result of the examination from the partition.

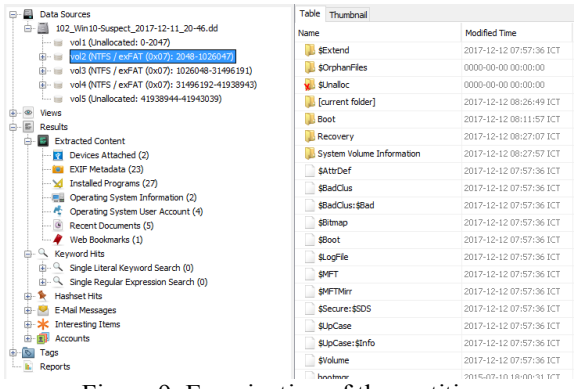


Figure 9. Examination of the partitions

There are five partitions in general, namely Vol1 until Vol5 but for Vol1 and Vol5 is unallocated space so only Vol2, Vol3, and Vol4 that contain the operating system and user data which can be examined. The results of the examination from the three partitions are summarized in Table 3 below.

Table 3. Results of the Examination

| No | Type of Findings | Function | Result |
|---|---|---|---|
| 1 | Vol2 | System Reserved | Can be examined |
| 2 | Vol3 | operating system data | Can be Examined |
| 3 | Vol4 | User data | Can be Examined |
| 4 | Recent Document | last files accessed by the user | Can be Examined |
| 5 | Deleted Data | The list of deleted data | Can be Examined |

The next procedure carried out is the analysis of digital evidence. The analysis is done by the limitations of the problems that have been determined that is the analysis of files previously deleted. Based on the findings on the partition volume 4, all the deleted data was detected by the tools. In this stage, it will be performed the procedure to restore the files that have been deleted. Autopsy provides features to perform the recovery. Four files performed the recovery process. File recovery results are placed on the Desktop folder to facilitate the recovery process.

From the results of the successful recovery, it can be seen that the deleted files are recovered successfully, and based on recalculating the hash code of the recovery file, and compared to the hash value of the file before it is deleted, the hash value is the same. This is proof that the deleted files have been successfully restored, successfully re-accessed, and are original files before they are deleted. Figure 11 below is the result of the calculation of the hash value of all four files that have been successfully recovered.

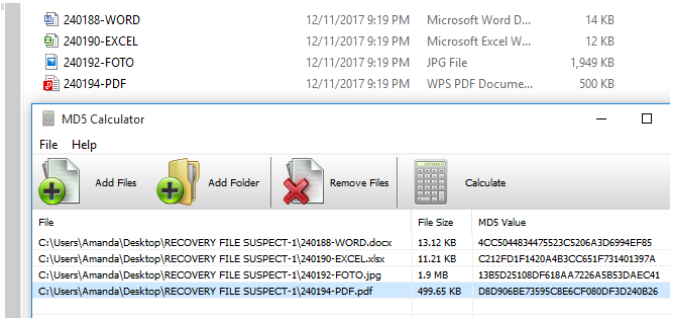

Figure 10. The value of the recovered hash file

## 4. CONCLUSION

The Acquisition System has been successfully used to carry out acquisition procedures on server virtualization Proxmox. From the results of the examination carried out, it was found that digital evidence resulting from the acquisition procedure that was carried out using the acquisition system can be read by forensic software. 100% the overall structure of files and folders which contain five partitions can be read. Also, the five files that have also been deleted 100% successfully restored. So based on some of these indicators, the acquisition process based on the live forensic method in the acquisition guide for SNI 27037:

2014 can be done on Proxmox server virtualization and the Acquisition System that was built successfully performs acquisition procedures following the standards. Then the acquisition system that has been produced is recommended for use by digital forensics investigators in handling cases against IAAS Cloud Computing model on Proxmox Server Virtualization.

## 5. REFERENCES


[1] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing-The business perspective. *Decision Support Systems*, *51*(1), 176–189.

[2] Columbus, L. (2017). Roundup Of Cloud Computing Forecasts. *Forbes*.

[3] Malhotra, L., Agarwal, D., & Jaiswal, A. (2014). Virtualization in Cloud Computing. *Information Technology & Software Engineering*, *4*(2), 2–4.

[4] Alqahtany, S., & Reich, C. (2016). A Forensic Acquisition and Analysis System for IaaS : Architectural Model and Experiment. *2016 11th International Conference on Availability, Reliability, and Security*.

[5] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, *5*(2), 235–247.

[6] Sudyana, D., Prayudi, Y., & Sugiantoro, B. (2019). Analysis and Evaluation Digital Forensic Investigation Framework Using ISO 27037 : 2012. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *8*(1), 1–14.

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

[8] Dykstra, J., & Sherman, A. T. (2012). Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing : Exploring and Evaluating Tools , Trust , and Techniques. *Digital Investigation*, *9*, S90–S98.

[9] Poisel, R., Malzer, E., & Tjoa, S. (2013). Evidence and cloud computing: The virtual machine introspection approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(1), 135–152.

[10] Digambar, P. (2015). *A Novel Digital Forensic Framework for Cloud Computing Environment*. Pilani: Birla Institute of Technology and Science.

[11] Lim, S., Yoo, B., Park, J., Byun, K., & Lee, S. (2012). A research on the investigation method of digital forensics for a VMware Workstation's virtual machine. *Mathematical and Computer Modelling*, *55*(1–2), 151–160.

[12] Wahyudi, E., Riadi, I., & Prayudi, Y. (2018). Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence. *International Journal of Computer Science and Information Security (IJCSIS)*, *16*(2), 1–7.

[13] Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices, and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056.

[14] Ahmed, W. (2016). *Mastering Proxmox - Second Edition* (2nd ed.). Packt Publishing.