SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037:2014

Didik Sudyana [1]
Department of Information Technology
STMIK Amik Riau
Pekanbaru, Indonesia
didik.sudyana@stmik-amik-riau.ac.id

Reza Tanujiwa Putra [2]
Department of Science and Technology
Universitas Islam Negeri Sultan Syarif Kasim
Pekanbaru, Indonesia
reza.tanujiwa.putra@students.uin-suska.ac.id

Soni [3]
Department of Information Technology
Universitas Muhammadiyah Riau
Pekanbaru, Indonesia
soni@umri.ac.id

***Abstract*—** Server virtualization technology has experienced significant development so that more and more industries are adopting this technology. By using server virtualization, the industry can make savings in purchasing new servers and maintenance because virtualization allows one server to run with multiple operating systems at once. The high level of use of virtualization raises a gap for the occurrence of computer crimes involving virtualization. When computer crimes occur on virtualization, it is necessary to conduct digital forensic investigations to find useful clues in solving crime cases. Therefore, in this study, a digital forensic investigation was conducted on Proxmox server virtualization by acquiring the entire storage virtualization media and carrying out checks on the results of the acquisition. Based on the investigation carried out, the acquisition technique by acquiring the entire storage media on Proxmox cannot be used because the structure of the evidence files and folders cannot be read perfectly.

Keywords—digital forensics investigation, traditional acquisition, server virtualization

I. INTRODUCTION

Current technological developments direct changes in the pattern of server usage in various industries which were originally based on one server for one need to be a server for many needs. To answer this need, virtualization server technology is the best solution.

According to [1] Server virtualization is a method that allows different operating systems to share the same hardware and run at the same time. The convenience of using server virtualization provides resource savings that can be done by industries such as saving new server purchases and saving maintenance costs [2]. Thus, this is the main reason why there is a significant increase in the number of industries that adopt server virtualization as support for business processes.

A higher level of adoption server virtualization has led to new crimes. Computer criminals began to commit crimes by involving server virtualization technology not only as a target but also as their main tool. To solve cases related to computer crime and find digital evidence which can be used as a guide to resolving cases, the scientific method known as digital forensics will be used [3].

The digital forensic approach is very appropriate to be used on the investigation process for resolving cases involving server virtualization, so research needs to be done with a digital forensic investigation approach on server virtualization, and knowing what type of digital evidence can be found in the server virtualization. However, when conducting an investigation, it must follow structured steps to guide the procedural verification [4]. There are several guidelines for conducting structured investigations, one of which is the Indonesian National Standard (SNI) 27037: 2014 concerning Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Therefore in this study will use the Indonesian National Standard 27043: 2014 as a structured reference stage.

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Currently, there are various kinds of server virtualization products. Proxmox is one of these products, but it has the main advantages from its competitors by having a free license which has almost same features as competitors. This is one of the reasons why many users choose Proxmox. So that this study will focus on Proxmox server virtualization.

II. LITERATURE REVIEW

A. *Digital Forensics*

Digital forensics is a method of collecting, preserving, analyzing, acquiring evidence and will later be presented in court [5]

The stages commonly used in digital forensic are[6] :

1) Collection: phase in collecting evidence
2) Examination: the initial phase of the examination based on the evidence found
3) Analysis: the search process for finding related evidence
4) Reporting: phase in giving conclusions from all phases

B. *Server Virtualization*

Server virtualization is a method that allows different operating systems to share the same hardware and makes it easy to move between operating systems and hardware virtualization. Different servers are partitions of a physical server to smaller virtual servers to help maximize server virtualization resources that contain the identity and number of individual physical servers, operating systems and processors. The server has a large number of benefits such as Hardware Utilization, Security and Development [7].

C. *Proxmox*

Proxmox VE is a debian linux based open source hypervisor operating system and can be used as an alternative to virtualization. Proxmox makes it possible to control multiple servers that are stored on one physical server. Proxmox consists of at least one physical server and some have several servers in it [8].

D. *SNI 27037:2014*

According to [9] SNI 27037:2014 is a digital forensics standard whose entire document is adopted from ISO 27037: 2012 with the reprint-publishing method. This SNI 27037: 2014 is a national standard that discusses specific guidelines related to digital forensic investigation activities. Which activities include identification, collection, acquisition and preservation. All of these processes are important processes that must be carried out carefully to maintain the integrity of the evidence. The methodology used in collecting digital evidence will affect whether or not the evidence is received in court. In addition to discussing digital evidence, SNI also discusses general guidelines on how to collect non-digital evidence. This standard can be used for the acquisition of digital devices such as:

(1) Digital storage media like a hard drive, floppy disk, optical and magneto-optical disks, and data devices with similar functions.
(2) Mobile phone, Personal Digital Assistance (PDAs) Personal Electronics Devices (PEDS), memory cards.
(3) Mobile navigator systems.
(4) Digital video cameras (including CCTV)
(5) A standard computer with network connections
(6) Network-based on TCP/IP and other digital protocols, and
(7) Devices with similar functions as above.

E. *Previous Research*

There are several studies that have been carried out previously related to server virtualization. [10] compare and analyze virtual images on virtualization that have been damaged to identify what has been added, removed and modified. [11] conducted a digital forensic investigation and made a method of recovering corrupted image files on the VMware workstation aimed at helping investigators conduct investigations. The next study was completed by [12] who made a comparison of the architecture, performance, and limitations of several types of VMs and saw which VMs gave good results for investigators. There are four types of VMs that are the object of research, namely Virtual Box, VMware Workstation, Cooperative Linux, & XEN Desktop. The other research [13], which produces research by ascertaining whether evidence of activities carried out and generated by virtual machines can be recovered or restored so that further checks can be made on Oracle Virtual Box. And finally a research was completed by [14] who made research in virtualization focusing on Virtualbox. The researcher were successful to analyze and recover a deleted virtual machine using autopsy and FTK tools.

III. RESEARCH METHODOLOGY

In this research, there are several steps taken, namely:

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

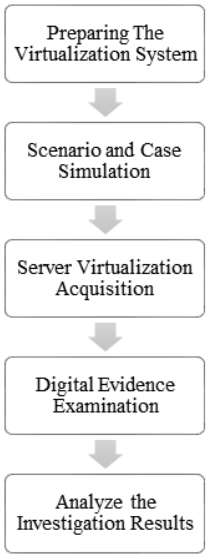

Fig. 1. The Steps of Research Methodology

(i) Preparing the Virtualization System is done by preparing infrastructure both hardware and software for Proxmox server virtualization which will be used as research objects.

(ii) In Scenario and Case Simulation, a computer crime case was created involving server virtualization with the Windows 10 virtual operating system. It was suggested that criminals used the Windows 10 virtual operating system and deleted some files indicated as evidence. There are 5 types of files with different file extensions that are deleted. The investigator will conduct an investigation to find evidence that has been deleted.

(iii) Server Virtualization Acquisition will be performed on Proxmox using dc3dd acquisition tools. In carrying out the acquisition procedure, SNI 27037: 2014 is used as a stage and guide for live forensic acquisitions where acquisitions are made when the server is still on.

(iv) Digital Evidence Examination is carried out using Autopsy forensic tools to view the structure of digital evidence and conduct an examination that focuses on finding files that have been previously deleted.

(v) Analyze the Investigation Results is the final stage where the analysis process is carried out on the findings obtained previously and draw conclusions from the analysis.

IV. RESULTS AND DISCUSSION

A. *Preparing the Virtualization System*

System preparation is done by preparing server virtualization infrastructure. The server specifications used as Proxmox and the software used are as follows:

Table 1 – Hardware and Software Specifications

No	Hardware / *Software*	Note
1	PC *Server*, Processor Intel Core i3-2100 CPU@3.10*Ghz*, Harddrive 80 GB, RAM 8 GB	Hardware
2	*Proxmox Virtual Environment* 4.3	*Server*
3	Linux Ubuntu Desktop 16.10	Virtual OS
4	Microsoft Windows 10	Virtual OS
5	*The Sleuth Kit Autopsy 4.1.1*	*Forensic Tools*

B. *Scenario and Case Simulation*

Case simulations are made on the Windows Virtual Operating System 10. Four types of files with different extensions are placed on drive E: \ then hashed the file. Extensions used are xlsx, jpg pdf, and doc. The hash file process is done to make the md5 hash value needed for the analysis process of evidence in the next stage using the MD5 Calculator software. The hash values of the four files can be seen in the picture below.

File	File Size	MD5 Value
E:\File Excel.xlsx	11.21 KB	C212FD1F1420A4B3CC651F731401397A
E:\File Foto.JPG	4.88 MB	3CE2ED99EE9C3A8BCBEB9A1003AE9BAA
E:\File PDF.pdf	809.72 KB	7AD588605366A029612767A049BCF440
E:\File Word.doc	371.5 KB	EDA5E784210964DAC966CF58A11C91F0

Fig. 2. Hash Value

After knowing the hash value of the four files, the procedure for permanently deleting files is done with the shortcut Shift + Delete.

C. *Server Virtualization Acquisition*

The acquisition procedure is carried out using the guidelines contained in the SNI 27037: 2014 document. The acquisition procedures listed in the document are as follows:

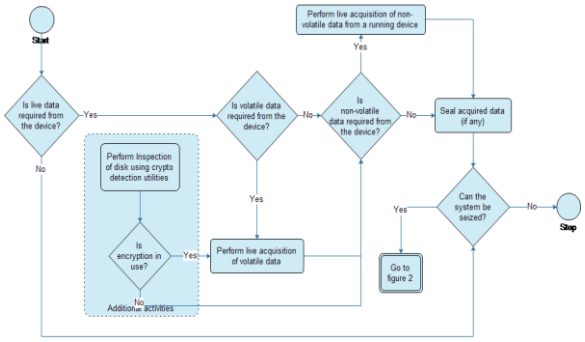

Fig. 3. The procedure of Live Acquisition

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

This stage was adjusted to the needs of the acquisition carried out on Proxmox server virtualization. Explanation of each step taken is:

(1) Data that will be acquired on Proxmox is live data. So that from Yes's answer continues to the next stage.
(2) Is volatile data needed? because only non-volatile data will be acquired, the choice is no.
(3) In the next stage is non-volatile data needed? In this study, non-volatile data is the main focus, so the answer "Yes" and continues to the stage of live acquisition for non-volatile data on a digital device that is on.
(4) At the stage of the seal acquired data, the hashing procedure uses MD5 on the acquisition file to do a seal on the data and verify it to ensure that the acquired file is the same as the original file
(5) The next stage is related to the seizure of evidence. In this study, electronic evidence in the form of a physical server is not carried out a seizure process so that the acquisition procedure is complete.

After mapping the stages of the acquisition plan, the acquisition process will then be carried out. The procedures and processes carried out in acquiring non-volatile data using dc3dd are:

(1) The process of mounting a USB drive is used as a storage medium for the acquisition of Proxmox physical servers. The mounting process shows that the USB drive is on the /dev/sdb drive.
(2) Next is the installation process of dc3dd software as a tool to carry out the acquisition process of Proxmox using "apt-get install dc3dd" on Proxmox terminal command.
(3) The last stage in the acquisition process is to carry out the acquisition process of all data on the proxmox hard disk and after the acquisition process is complete, the hashing process is carried out on the acquisition results file. The hash value of md5 from the hashing process can be seen in the picture below.

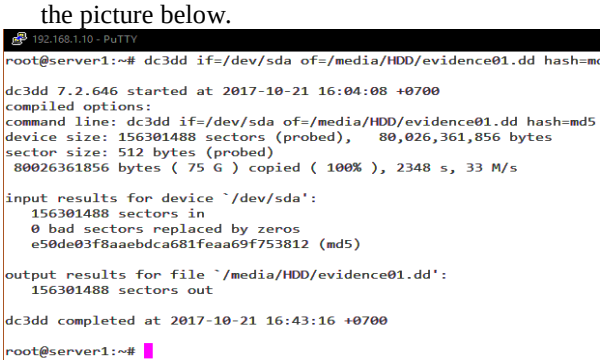

Fig. 4. The Acquisition Process and Hash Value

D. Digital Evidence Examination

This process was carried out to extract data from the acquisition and then look at the structure of files and folders from the digital evidence obtained from the acquisition using the help of Autopsy forensic tools. Figure 5 until Figure 10 below is the result of an examination.

Fig. 5. The Result of Examination (1)below is the result of an examination of vol1 where only one file was found.

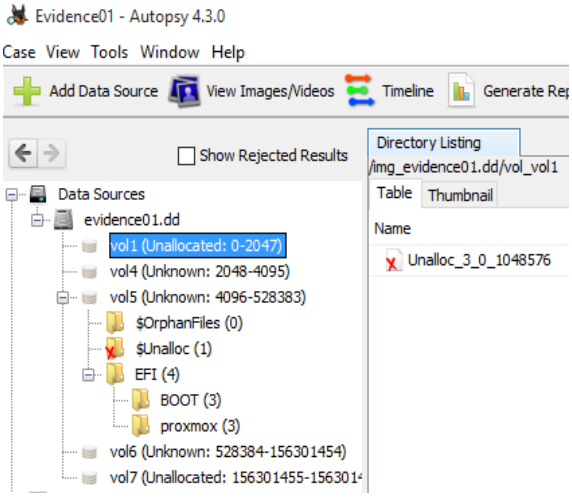

Fig. 5. The Result of Examination (1)

Fig. 6 below is the result of an examination on vol4 where only one file was found.

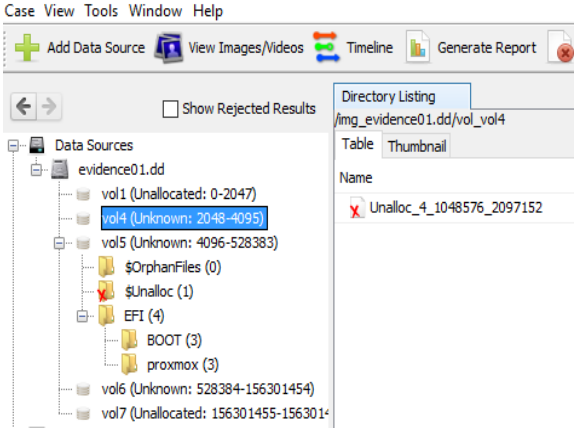

Fig. 6. The Result of Examination (2)

Fig. 7 below is the result of the examination process on vol5 and found 8 files and 5 folders.

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

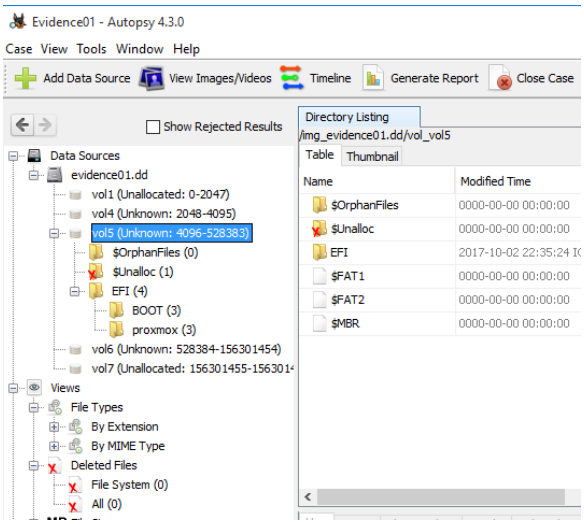

Fig. 7. The Result of Examination (3)

Fig. 8 below is the result of vol6 examination where only one file is found.

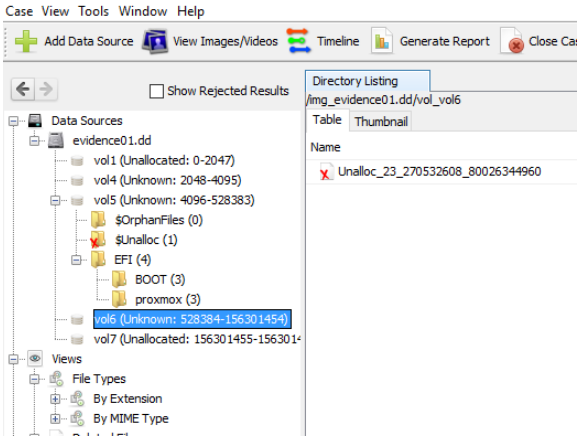

Fig. 8. The Result of Examination (4)

Fig. 9 below is the result of an examination in vol6 where on vol7 there is only one file found.

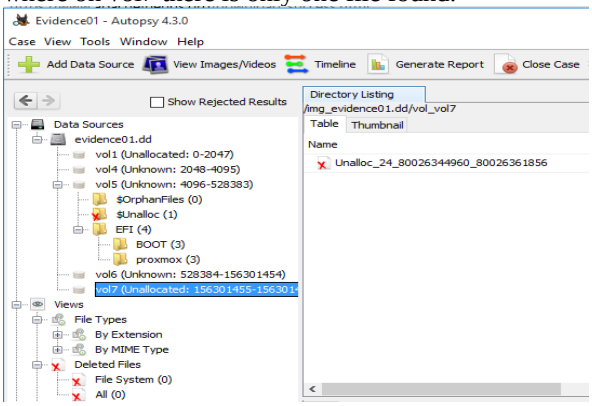

Fig. 9. The Result of Examination (5)

Fig. 10 below is the result of an examination of deleted files and has been grouped by Autopsy where in this case were not found any files that can be performed recovery procedures.

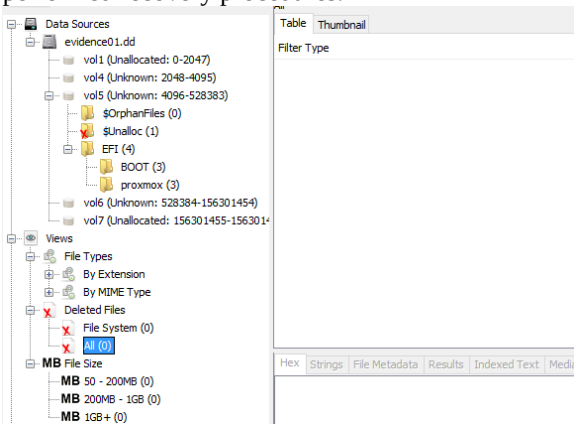

Fig. 10. The Result of Examination (5)

E. Analyze the Investigation Results

From the results of the investigation, it did not succeed in finding Windows 10 data or partitioning the virtual operating system, either Windows 10 or Ubuntu Linux. So that previously deleted files cannot be found and performed recovery procedures.

Based on these findings, the process of digital forensic investigation of Proxmox server virtualization cannot be done because the found file and folder structure cannot describe the entire content on the Proxmox server hard drive as evidence so that the analysis process cannot be continued to obtain information as a guide to the investigation.

V. CONCLUSION

From the results of the examination carried out, there was no Windows 10 partition or Windows 10 data found. Also, it was not able to find the deleted files. Based on the results of this examination, it can be concluded that the general acquisition procedure carried out by acquiring all hard disk data using dc3dd on Proxmox server virtualization cannot be used. Because the acquisition results obtained, cannot read the data on the Windows 10 partition and find the data that has been deleted.

The analysis that can be concluded related to the cause of not finding the required evidence, is due to the acquisition process using a traditional model by acquiring the entire storage media on Proxmox. The traditional acquisition model failed to find the virtual operating system partition contained in the storage media.

So that further research needs to be done to find the right acquisition technique for the virtual operating system that is the target of the investigation. The acquisition technique for further research can be

Journal Publications & Informatics Engineering Research
Volume 3, Number 2, April 2019
DOI : https://doi.org/10.33395/sinkron.v3i2.10029
e-ISSN : 2541-2019
p-ISSN : 2541-044X

done by focusing only on virtual drives that have operating systems that are subject to investigation.

REFERENCES

[1] R. Kumar and S. Charu, "An Importance of Using Virtualization Technology in Cloud Computing," *Glob. J. Comput. Technol.*, vol. 1, no. 2, pp. 56–60, 2015.

[2] E. Ali and D. Sudyana, "Virtualization Technology for Optimizing Server Resource Usage," *Int. Conf. Eng. Technol. Dev.*, vol. 2, no. 1, pp. 208–212, 2014.

[3] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037:2014," *J. Inform. Sunan Kalijaga*, vol. 1, no. 2, pp. 75–83, 2016.

[4] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," *Semin. Nas. SENTIKA*, vol. 2014, no. Sentika, 2014.

[5] A. Agarwal, M. Gupta, and S. Gupta, "Systematic Digital Forensic Investigation Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–134, 2011.

[6] S. Rani, "Digital Forensic Models□: A Comparative Analysis," *Int. J. Manag. IT Eng.*, vol. 8, no. 6, pp. 432–443, 2018.

[7] V. Soundararajan and K. Govil, "Challenges in building scalable virtualized datacenter management," *SIGOPS Oper. Syst. Rev.*, vol. 44, No. 4, pp. 95–102, 2010.

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

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

[10] M. Hirwani, Y. Pan, B. Stackpole, and D. Johnson, "Forensic Acquisition and Analysis of VMware Virtual Hard Disks," 2012.

[11] 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.

[12] F. M. Patterson, "The Implications of Virtual Environments In Digital Forensic Investigations," University of Central Florida, 2013.

[13] C. Neal, "Forensic Recovery of Evidence From Deleted Oracle Virtualbox Virtual Machines," no. December, 2013.

[14] E. Wahyudi, U. I. Indonesia, I. Riadi, U. A. Dahlan, Y. Pray, and U. I. Indonesia, "Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 2, pp. 1–7, 2018.