

Analysis of Virtual Machine in Digital Forensics

Jenita Ann Mathews¹, Glenis P George², Dhanalakshmi M P³

¹ Student, Dept. of Computer Science, ER & DCI Institute of Technology, Trivandrum, Kerala, India

² Senior Engineer, Knowledge Resource Centre, CDAC, Trivandrum, Kerala, India

³ Assistant Professor, ER & DCI Institute of Technology, Trivandrum, Kerala, India

Abstract - *With the advancement in virtualization technology, the use of virtual machines has been increased. A virtual machine also known as guest operating system can perform as an actual system and works as a normal computer and provides the complete functionality of an operating system to the user. As the popularity and the use of virtual machines increases, crimes involving them are also on the rise. The wide use of virtualization technology is becoming a new challenge for digital forensics. However, where there is any new technology for good purpose, there is always its illegitimate usage as well. Virtual Forensics is a new trend in the area of digital forensics. The analysis of virtual machine monitor and associated virtual machine files is of utmost importance. This project proposes a sound forensics methodology to acquire and analyze the virtual machine files by utilizing the VMware and Oracle Virtual Box artifacts.*

Key Words: Virtualization, Virtual machine, Digital Forensics, VMware, Oracle Virtual Box

1. INTRODUCTION

The concept of virtualization is taken from mainframe days of late 1960s and early 1970s. The company IBM spent a lot of time and effort in developing the shared usage of computer resources among a large group of users. The best way to improve the resource utilization is through the virtualization. Virtualization is a technology that enable multiple operating systems to run on a single host system. A software called hypervisors separate the physical resources from the virtual environments. There are two types of hypervisors, type 1 and type 2 hypervisor. VMware ESX/ESXi, Citrix Xen Server are examples of Type 1 hypervisor. Examples of type 2 hypervisors are VMware workstation, Oracle VirtualBox [1].

With the modernization in computer hardware and increase in processing powers of CPU, the use of virtual machines is on its peak. A virtual machine is a software implementation of a computer and executes programs like a host system. It uses physical resources of the host system on which it runs. Therefore, it is highly needed to understand this technology thoroughly from forensic point of view. The virtual machine can be used for both legitimate and illegitimate use. Legitimate use can be Software Testing, malware analysis, backups and disaster recovery of data centers or any research and development purpose [2]. Illegitimate use is when the virtual machine is used to perform any sort of criminal activity. That can be

cybercrime, copyright infringement, money laundering, identify theft, child sexual abuse, pornography, and cyber terrorism etc.

Digital forensics is a sequence of process of identifying, obtaining, analyzing and presenting evidences to the court to resolve a criminal case by observing and maintaining the integrity and authenticity of the evidence. With the advancement in virtualization technology virtual machines are becoming a subject of interest [10]. The applying of digital forensics in virtual machines is called as virtual machine forensics. Virtual machine is select as a good platform for committing crimes because of its hiding nature. Virtual machine is used as a forensic evidence to obtain valuable data. The analysis of virtual machine monitor and associated virtual machine files are significant in virtual machine forensics.

Oracle Virtual box VM (virtual machine) software is used to create virtual machines in this project. The virtual hard disk file is analysed to retrieve all its contents. A user's activity trail is recorded in the virtual machine is an important digital evidence in terms of digital forensics. The VMware workstation and oracle virtual box generates each virtual machine image, snapshot file, log and configuration file. Therefore, these files should be checked. This project proposed to analyse the evidences left by an attacker. This evidence will be helpful for the law enforcement to find the final suspect.

2. LITERATURE SURVEY

Virtualization technology paved the way for the growth of virtual machine forensics. The authors of the paper [2] focused the forensic analysis of VMware virtual machine in forensics and anti-forensics model. The analysis of virtual machine is done when anti-forensics measures are taken to hide or destroy the evidence in virtual machine. A damaged virtual machine disk image is complex to examine because of the structural characteristics. Therefore, author of [3] have suggest an investigation procedure of digital forensics and data recovery method on the damaged virtual disk images of VMware Workstation. The live acquisition method to acquire the virtual machine files from the host system and analyse the raw data stored in the grains is described in the paper [4]. G. Dorn and S. Conrad [5] analyses the impact of a virtual machine on a host machine. They discussed the trace evidence related to the installation and execution of virtual machines on a host machine. It provides useful information about the types and locations of files installed by

virtualization software, the processes and artifacts created by running virtual machines. The author of the paper [10] presented the forensic acquisition of virtual disk and the snapshot comparison analysis.

3. PROPOSED SYSTEM

The block diagram of the proposed system is shown in Fig. 1. The block diagram of the proposed system is divided into three phases. The first phase is the detection and acquisition module. This involves the identification of virtual machines in the host system. By acquisition, the process of obtaining a binary bitwise copy of the entire contents of all digital media that are identified. The acquired evidence is preserved and standard hash signatures like MD5 or SHA1 is used to verify integrity of the digital evidence. The analysis phase module contains the analysis of virtual disk, log file, snapshot and configuration files. The third phase is reporting. It summarizes and provides explanation of conclusions.

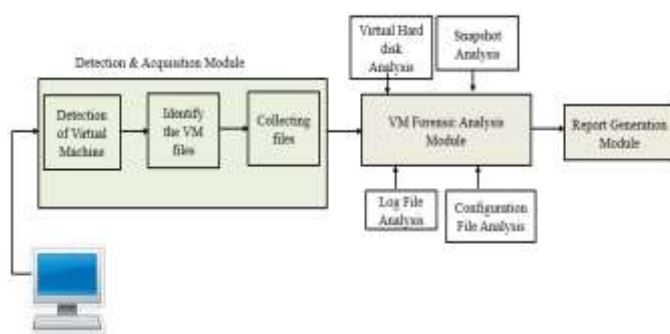


Fig.1: Block Diagram of Proposed System

4. SYSTEM STUDY

Virtual Disk Image (.vdi) is the disk image created by Oracle Virtual Box. VDI is a method to create a copy/image/replica of a virtual machine’s hard disk to be later used for disk backup, restoration or copying to a new virtual machine. VDI files are written in little endian format. The VDI has four sections:

- A 72-byte pre header
- A standard header descriptor. This is following by padding to the next 1MB boundary (*).
- An image block map. If the (maximum) size of the virtual HDD is N MByte, then this map is 4N bytes long. Followed by more padding to the next 1MB boundary.
- Up to N x 1MByte image blocks.

5. SYSTEM DESIGN

The system design includes the architecture diagram of the proposed system. This architectural diagram consists of three tiers. The three tiers are presentation layer, logical

layer, Data Access Layer. Fig. 2 shows the architecture diagram of the proposed system. The presentation layer is the top most layer of the system. It contains the graphical user interface, which is the layer that having direct connection with the user. It is the interface that includes the analysis viewer and report viewer. Analysis viewer gives the result of the analysis module and report viewer gives the detailed report.

The logical layer is the layer in which the applications or activities done by the system are represented. This tier consist of different basic modules. Detection of Virtual machines from the host machine, VMWare VM log file analysis and the Oracle virtual Box Virtual Machine File Analysis. Each file is analyzed and the result is given to the analysis viewer.

The third tier is the data layer. The data layer consists of the database management module. This layer contains all the virtual machine files in the VMware and Oracle Virtual Box.

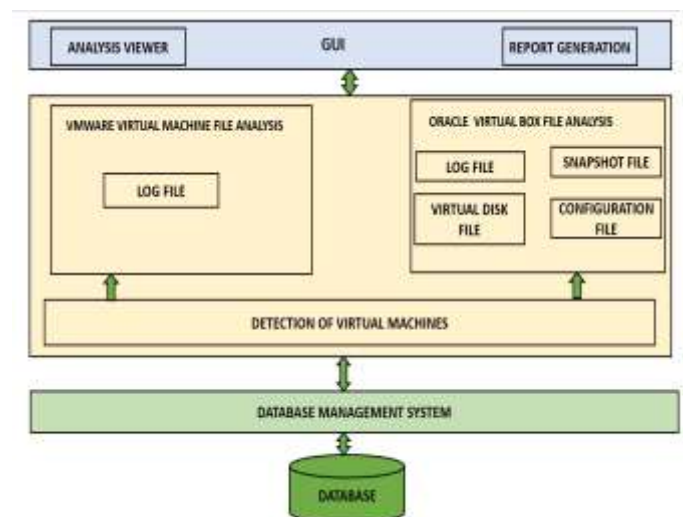


Fig. 2: Architecture Diagram

6. IMPLEMENTATION

The proposed system in this paper is implemented using python 3.7 scripting language. Python has built-in capabilities to support cyber investigations and perform forensic analysis. Python play an important role in digital forensics. Python is a popular programming language and is used as tool for cyber security, penetration testing as well as digital forensic investigations. When the investigator select python as the investigation tool for digital forensics, he need not need any other third party software for completing the task. Some of the unique features of python programming language that makes it good for digital forensics projects are simplicity of syntax, comprehensive inbuilt modules, cross platform compatible, provides various modules and functions. The host and guest operating system used in this paper is windows 10.

The hardware and software requirements for this research work is given in table 1.

Table 1: Hardware and Software Requirements

Hardware	Software
Processor: Intel Core i3 or above	OS: Windows 10
Speed: 1.3Ghz	Oracle Virtual Box6.0
RAM: 4GB	VMware Player 15.5.1
Disk: 10GB or more	Anaconda 3-5.3.1
	Python 3.7
	Spyder 3.3.4

7. ANALYSIS AND RESULTS

7.1. Detection of Virtual Machine

Investigator wants to check whether any virtual machine installed in the host machine. If he clicks the detect button, installed virtual machines are detected. Fig. 3 shows the GUI of detection phase. Fig. 4 and 5 show the virtual machines of the Oracle Virtual Box and VMware respectively.

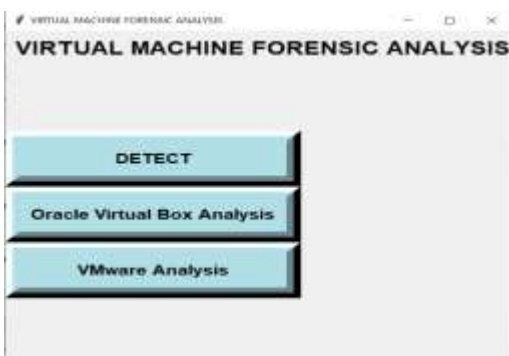


Fig. 3: GUI of the proposed system

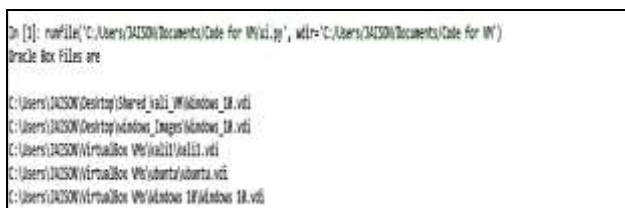


Fig. 4 : Oracle Virtual Box Virtual Machines



Fig. 5 : Vmware Virtual Machines

7.2 VMware Log File Analysis

Log file gives the information about the version of the VMware player software. It provides the host operating system, host system name and its specifications where the VMware player is installed. Log file of any virtual machine has a record of previously installed ISOs and showing the locations of previous ISOs. VMware log provides the details of connected USB devices. The list of connected USB devices that connected with the system at different times can also be seen from log files. Log contains the USB Disk name along with its connection date/time and serial number of USB. Fig. 6 presents the output of VMware log file.



Fig. 6 : Output of VMware Log File

7.3 Oracle Virtual Box Log File Analysis

Fig. 7 presents the GUI of Oracle Virtual Box Forensic Analysis. There are four log files are created in the oracle virtual box. Selectorwindow.log, VBoxSVC.log, VBox.log, VBoxhardening.log are the log files. Two of them are created at the time of installing the virtual box software. This is common to all virtual machines. Other two are separate for each virtual machine.

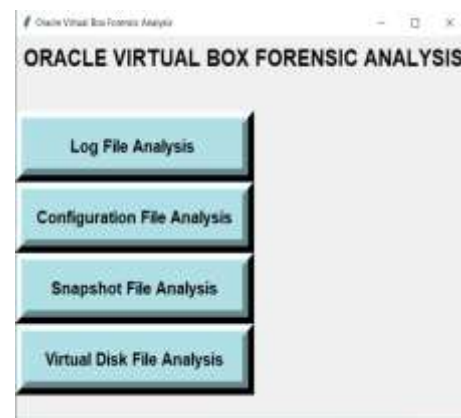


Fig. 7: GUI of Oracle Virtual Box Forensic Analysis

i. Selectorwindow.log

This log file provides the information of virtual box installed date and time, last vm opened, host OS, host system product version, host RAM total space and available free space. process running behind the selector window is Virtual Box.exe. The fig.8 shows the output from the selectorwindow.log.

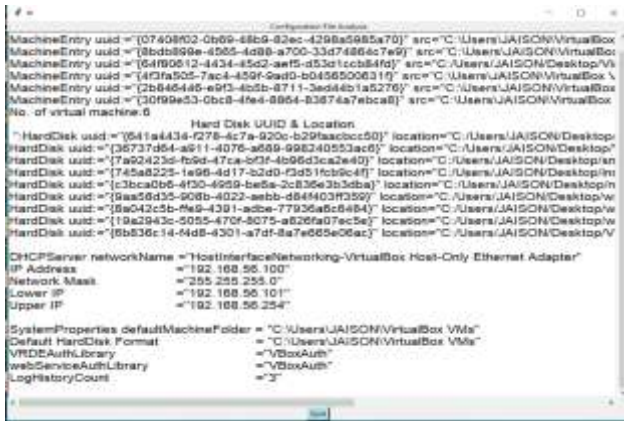


Fig. 13: Output of Xml file.

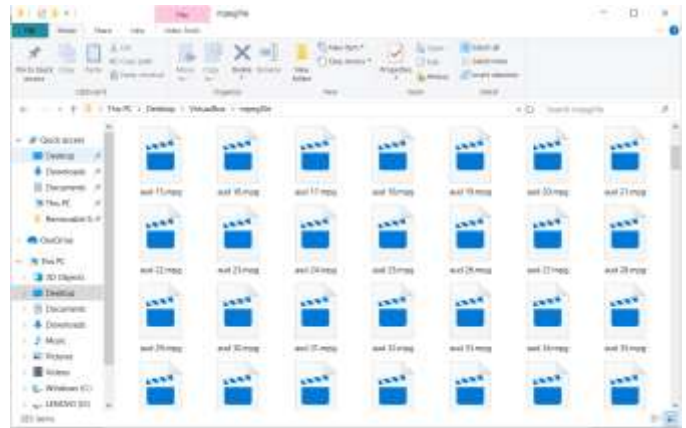


Fig. 16: MPEG Files Carves

7.5 VDI File Analysis

The VDI file contains a header section. The header of the VDI file is decoded and it provides the VDI header provides the information of file signature of VDI file, Version, header size, disk type, offset block, offset data, sector size, total block size in MB, total block count and the total allocated block count. VDI header decoded output is shown in Fig. 14.

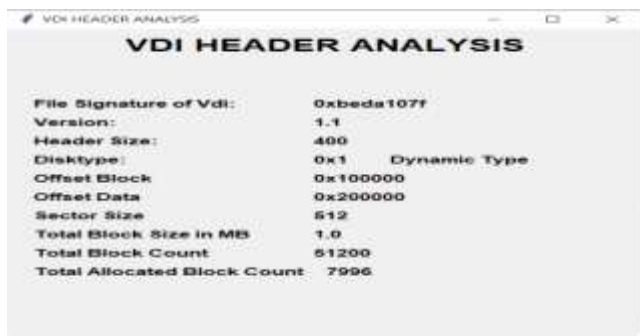


Fig. 14: VDI header

The jpeg and mpeg files are carved from the vdi file. Nearly 1592 jpeg and 282 mpeg files are carved from the vdi file which shown in Fig. 15 and 16.

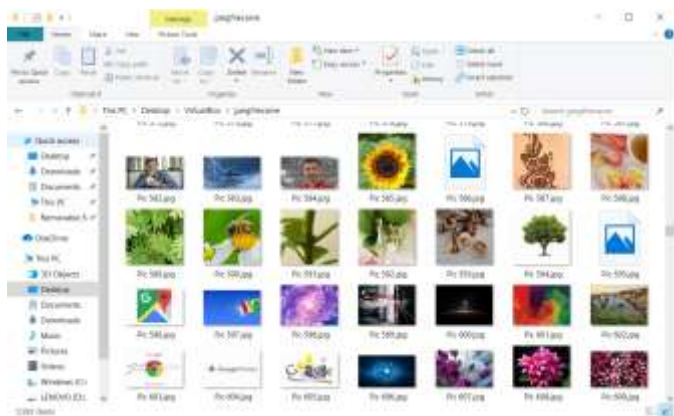


Fig. 15: JPEG Files Carves

In Kali linux, there is a file carving module called foremost, carved the other files such as avi, bmp, dll,exe, gif, htm, ole, png, wav, wmv etc. Output is shown in Fig. 17.



Fig. 17: Output of VDI File

The analysis shows the evidence that google chrome is installed in the windows 10 virtual machine and it was used for web browsing on the virtual machine. The details of the web browser history, web cookies, web accounts, web downloads are get from the vdi file. The results showing that the user enter websites google, yahoo login page and some images are downloaded in the virtual machine. The information such as web search results, URLs, date and time accessed, email id of the user is got from the analysis of vdi file which is shown in Fig. 18. Web cookies result is exhibited in Fig. 19.

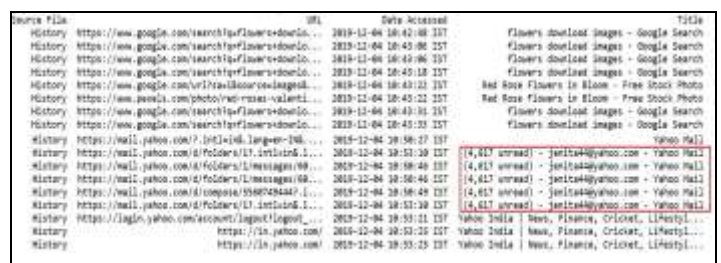


Fig. 18 : Web Search Results



Fig.19 : Web Cookies results

7.6 Snapshot File Analysis

For snapshot analysis, two snapshots are needed. A clean snapshot of the VM before the activity and a snapshot after the activity is needed. Two snapshots are compared using the md5 hash values. Fig. 20 shows hash value comparison.

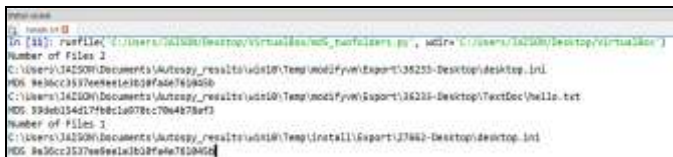


Fig. 20: Hash Value Comparison

The difference between snapshot vdi file and normal vdi file is identified by looking at the offset 0x4C, the disk type is 04 it is snapshot and 01 it is normal VDI with dynamic disk type.

8. CONCLUSIONS

The recognition and understanding of virtualization software and virtual machine play an important role in digital forensics investigations. There are a lot of artifacts are produced during the creation and execution of virtual machines. This paper clearly presented the analysis of log file, configuration file, snapshot files and the virtual disk files of the Oracle Virtual machine. It also provides a detailed analysis of VMware log file.

Based on the results which was obtained in the analysis of virtual machine and its associated files it can be concluded that the user activity trail can be found. A browser history analysis was carried out in the virtual machine to show that the activities of the user done in the website.

REFERENCES

[1] H Lee, "Virtualization Basics: Understanding Techniques and Fundamentals," School of Informatics and Computing, Indiana University 815 E 10th St. Bloomington, IN 47408, December 2014.

[2] Hammad Riaz, Mohammad Ashraf Tahir, "Analysis of VMware Virtual Machine in Forensics and AntiForensics Paradigm", 6th International Symposium on Digital Forensic and Security, July 2018

[3] S Lim, B Yoo, J Park, K Byun, S Lee, "A research on the investigation method of digital forensics for a VMware Workstation's virtual machine," Mathematical and Computer Modelling, Volume 55, Issues 1-2, January 2012, Pages 151-160

[4] V. Meera, M.M. Isaac, C. Balan, "Forensic acquisition and analysis of VMware virtual machine artifacts", IEEE International MultiConference on Automation Computing Communication Control and Compressed Sensing (iMac4s), pp. 255-259, 22-23 March

[5] G. Dorn, C. Marberry, S. Conrad and P. Craiger, "Analyzing the Impact Of A Virtual Machine On A Host Machine," Advances in Digital Forensics V, Fifth International Conference on Digital Orlando, Florida, USA, January 26-28,2009

[6] Saumya Awasthi and Ajay Pratap, "A Virtual Environment Forensic Tool", International Journal of Cyber-Security and Digital Forensics, Volume 7 Issue 1, pp.63-71, April 2018.

[7] Smita V. Khengar, G. H. R. C. E. Nagpur, and Rajiv V. Dharaskar, "Digital Forensic Investigation for Virtual Machines", International Journal of Modeling and Optimization, Vol. 2, No. 6, pp. 663-664, December 2012

[8] M. Hirwani. Y. Pan. B. Stackpole. D. Johnson, "Forensic Acquisition and Analysis of VMware. Virtual Hard Disks," 2012 Rochester Institute of Technology, Accessed from <http://scholarworks.rit.edu/other/297>

[9] Manjaiah D.H, Ezz El-Din Hemdan "Digital Forensics in Virtual Environment" CSI Magazine, March_2016.

[10] ShaguftaRajguru, AayushPathak, Danish K. Chaus, Akshay J. Boramani "Design of Tool for Digital Forensics in Virtual Environment" International Journal of Computer Applications, Volume 163 - No.4, April-2017