iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5335

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Forensic Acquisition and Analysis of Deleted Vmware Virtual Machine

Ankita Sojitra[1], Dr.Ravi K Sheth[2]
[1]*Department of Information and Technology Raksha Shakti University, Ahmedabad, India*

Abstract: ***Virtual machine forensics plays very important role now a days. It is a one type of software that behaves like a physical computer. VMware Workstation allows users to set up and use virtual machines simultaneously with the actual machine on a single physical machine. Perhaps the most pressing concern in any digital investigation is the issue of virtual machine volatility. The complexities of virtual hard drives for data recovery are not fully addressed by the current digital forensic tools. For this reason, it is necessary to investigate ways of capturing evidence other than using current forensic digital methods. Forensics tools are not able to recover a deleted VMware files. In this report to show how to find deleted VMware from the existing system and also find how to get back that local deleted files from the VMware machine.***
Keywords: VMware forensics, Virtualization, Virtual machine, VMDK file format

I. INTRODUCTION

Virtualization is the creation of flexible replacements for actual resources- replacements that have the same functions and external interfaces as their actual but counterparts differ in size, performance, and cost attributes. One of the advantages of virtual machines is the ability of a virtual machine to operate on almost any underlying configuration of hardware and software. Virtual machines can be shared and duplicated for many purposes, such as software testing. Moreover, one host machine can run multiple VM guest machines simultaneously. Within the actual machine host, the VM application-guest runs its own self-contained operating system. This virtual machine can be used for almost any design variant. It can be described more simply as a virtual computer that runs on a physical computer. In this way, virtual machines can be shared and duplicated for many purposes, such as software testing. Moreover, one host machine (the actual system) can run multiple VM guest machines simultaneously. Educational institutions can use virtual machines to teach a variety of topics and information technology courses. Many different operating systems can be demonstrated on a single student desktop, which requires little time to set up the systems. The benefits for the students are more instruction and hands-on in a shorter period of time. The focus will be on virtual machine uses for the scope of this paper as it relates to forensic analysis, with both a virtual machine as your evidence and as an asset to your forensic tool box. Virtualization involves a shift in physical to logical thinking, treating IT resources rather than separate physical resources as logical resources.

You can consolidate resources such as processors, storage, and networks into a virtual environment using virtualization in your environment that provides the following benefits like Consolidation to reduce hardware cost, Workload optimization, Flexibility in information technology and responsiveness. VMware, a division of Dell Technologies develops and sells VMware Workstation. VMware Workstation is a host hypervisor that runs x64 versions of Windows & Linux OS. Each virtual machine, including versions of Microsoft Windows, Linux, BSD and MS-DOS, can run its own operating system. A free non-commercial version, VMware Workstation Player, is available. An operating system license is required to use owners such as Windows. Ready-to-use VM VMs are available in various sources, configured for different purposes. VMware Workstation includes the ability to group multiple virtual machines into an inventory folder. The machines can be activated and disabled as a single object in such a folder, which is useful for testing complex client-server environments.

II. LITERATURE REVIEW

Juan Carlos Flores Cruz, Travis Atkison, conducted research on a forensic virtual investigation into some of the methods and techniques used to acquire, authenticate and analyse a virtual forensics machine. The main steps mentioned in this paper to conduct an efficient forensic research on a host machine are forensic image creation, sensitive identification and information recovery, virtual machine analysis and documentation. Hammad Riaz, Mohammad Ashraf Tahir it shows in this paper that the typical nature of virtual machine analysis. As with most forensic tools, there is no automatic decoding of vmdk and other types of virtual machines created by different hypervisors. Most of the time, these forensic tools only display these virtual machine disk files in the file extension list identified. However, in the list of total discovered files, forensic analyst must manually check the presence of these

files. Although the present of VM in the disk image is signaled by some forensic tools, even then the analyst must perform separate analysis of that virtual machine.

Manish Hirwani, Yin Pan, Bill Stackpole and Daryl Johnson This paper presents the acquisition and analysis of VM hard drives. For analyzing VM snapshots and vmdk files, a forensic tool is being developed and has been shown to be forensically sound. The authors studied solutions for acquiring and analyzing live virtual machines based on VM files. For the acquisition of virtual disk images, a forensically sound process is provided. A snapshot analysis tool, Forensics Snapshot Analysis, was also developed. For researchers in forensics, analyzing hard disk images from VM and presenting relevant evidence in court is a powerful tool. In response to incidents, this tool may also be useful for confirming an infringement and carrying out further forensic analysis. It is possible to further study the effect of encrypted files and volumes on the analysis carried out by this tool. To handle other file systems such as FAT, NTFS and other file systems, changes can be made to the developed tool.

Meera V, Meera Mary Isaac, Balan C This paper discusses how live acquisition from the host OS can be accomplished to acquire files related to the VM. The paper also describes how these acquired files can be analyzed in order to obtain raw data stored in different grains. Methods to assist forensic examiners support the study by providing valuable information from the raw data from different grains pointing to grain table entries. There is a growing prevalence of cybercrimes, so forensic experts are eagerly hunting for cyber space victims. Cybercrime syndicates are using virtual machines to engage in heinous conspiracy to achieve lucrative goals.

III. VMWARE VIRTUAL MACHINE ANALYSIS

VMware is a well-known virtual machine (VM) software vendor and owns a large part of the market. VMware's products include, among others, VMware Workstation, VMware Server, and VMware ESXi. VMware, a Dell Technologies division, is developing and selling VMware Workstation. There is a free version for non-commercial use, VMware Workstation Player. An operating system license is required to use the owners, such as Windows. Ready-to-use VM VMs are available in various sources, configured for different purposes. At any time, VMware Workstation Pro can save a virtual machine's status snapshot. These snapshots can later be restored, effectively returning the VM to the saved state as it was after the VM snapshot and free of any damage. As VMware defines, virtualization is "the process of creating software-based representations of something rather than a physical one"

Extension	File Name	Description
.log	<vmname>.log	This is the file that tracks the key activity of VMware Workstation. This file can be useful to solve problems in case of problems. This file is stored in the directory that contains the configuration file (.vmx) of the virtual machine.
.nvram	<vmname>.nvram	This is the file that stores the BIOS status of the virtual machine.
.vmdk	<vmname>.vmdk	This is a virtual disk file that stores the contents of the hard disk of the virtual machine. If the virtual machine is directly connected to a physical disk instead of a virtual disk, the.vmdk file will store information about the partitions that are permitted to access the virtual machine.
.vmem	<uuid>.vmem	The paging file of the virtual machine, which backs up the main memory of the guest in the host file system. This file exists only when the virtual machine is running or if the virtual machine has been blocked.
.vmss	<vmname>.vmss	This is the suspended state file, which stores the status of a suspended virtual machine Some earlier VMware products used the .std extension for suspended status files
.vmsd	<vmware>.vmsd	A VMSD file contains the metadata about the snapshot.
.vmx	<vmname>.vmx	This is the main configuration file, which stores the configuration chosen in the New Virtual Machine Wizard or in the virtual machine configuration editor. If you created the virtual machine with a previous version of VMware Workstation on a Linux host, this file could have a .cfg extension
.vmxf	<vmname>.vmxf	This is a complementary configuration file for virtual machines located on a computer. Note that the .vmxf file remains if a virtual machine is removed from the computer.

Table 1: File of VMWare Virtual Machine

Vmware virtual machine basically used vmdk file for data stoagre. The VMDK file extension is associated with the specifications used with the VMware virtual machine files for disk format virtual machine. VMDK was originally developed by VMware but is now an open file format, competing with the Virtual Hard Drive Format of Microsoft and not directly compatible with both. To facilitate the conversion process, third-party tools such as the VMDK to VHD converter are available. When some files are deleted from the virtual machine or virtual machine is being corrupt then there may chances to loss of data.

IV. ANALYSIS OF THE RESULTS

In this paper, the information that was retrieved from the virtual machine is in different-different test cases. First take forensic images of where exactly your virtual machine is being installed.

Use the FTK imager to extract that VM from the image of the host drive. Most analysts have confusion about vmdk's analysis that it must first be imaged before being analysed in any forensic tool such as FKT toolkit ,FTK Imager or Encase etc. Suppose the size of that virtual drive is selected as 60gb when creating a Virtual machine and the option ' allocate full capacity ' is not selected from advanced options. A partition size of 60gb would be displayed in Guest OS after installation of Guest OS. Whereas if the size of the same virtual drive is checked in the Host OS, it would be between 10gb & 12gb depending on the Guest OS i.e. Windows7, Windows10 and so on. Take image of drive then get virtual machine of your system for example windows7. VMware's presence in installed programs also indicates the likely presence of any virtual machine inside the suspected hard drive. VMware defaults to 'C:\Program Files(86)\VMware\VMware Workstation.' It's always important to check Virtual Machines' default location. It varies depending on the operating systems of the host. For instance, it is ' C:\Users\username\Documents\Virtual Machines\guestOSname ' in Windows 10. Now with the help of image open in FTK imager & open that drive image in this. At above location find the deleted symbol on the virtual machine if it is deleted. Or is any change in that vm then also it indicate that. Here take image for delete of files from a virtual machine. Then now it not possible to take it with normal procedure. So here is method to take that data. For according condition try with Testdisk. First take that vmdk file or vmx file which can be remove or delete. Open vmware and this virtual machine with .vmx file. Its not compulsory to have samre file location. But it find all directory to install that are correct, open that machine then install testdisk on that created virtual machine and get results.

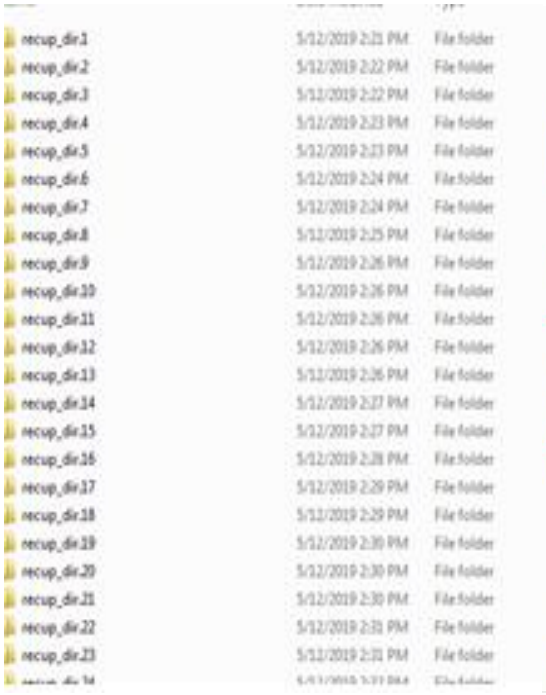


Fig-1 retrieved delete data by folder

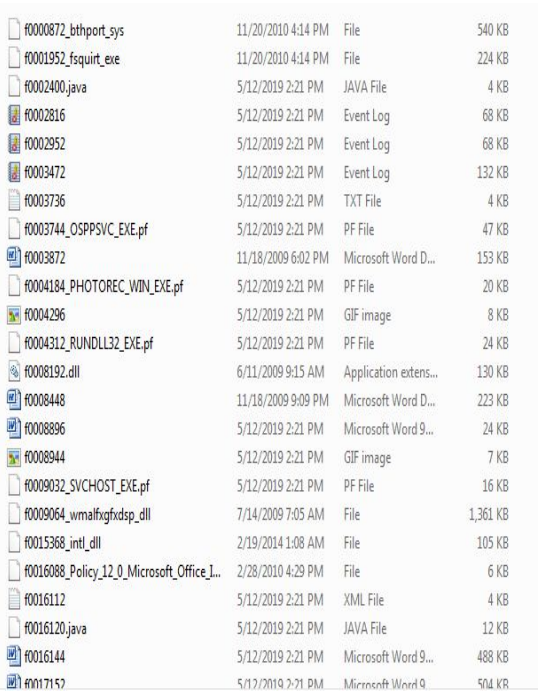


Fig-2 doc file that are deleted.

For second case virtual machine that are present in VMware but some files are deleted from that then also above method is useful directly in system can get data with this the data are not in same name format. check it by hex editor to compare the values of files that are deleted. It possible with any guest OS.

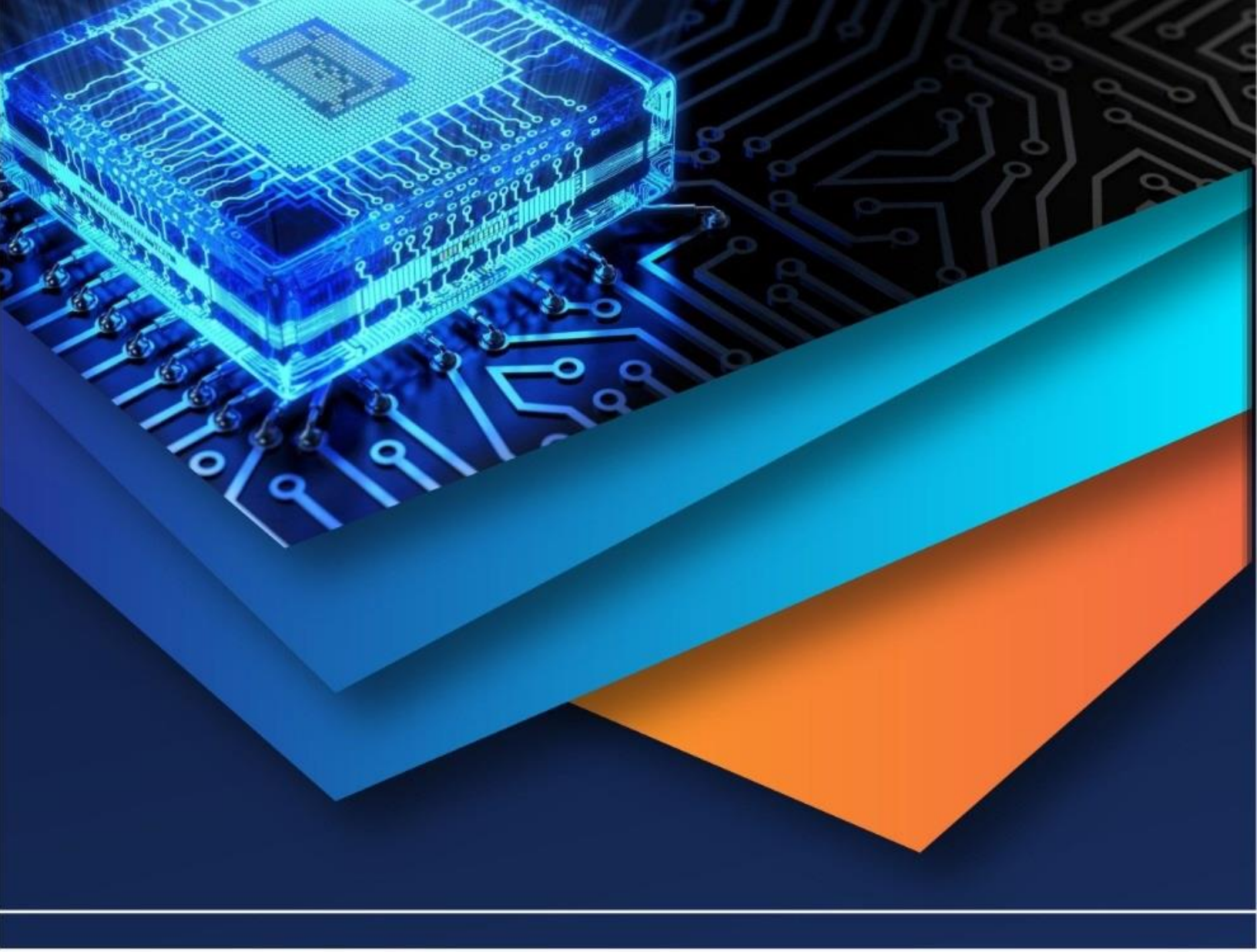
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

V. CONCLUSION AND FUTURE WORK

There are many methods available to recover a data or corrupted files from a hard drive but in VMware it's difficult because the data storing structure of VMware is quite different from regular hard disk. The analysis of virtual machine is typical in nature. As most forensic tools, vmdk and other types of virtual machines created by different hypervisors are not automatically decoded. The normal basic virtual machine can only get 2gb data from a disk.so may store another data in a unallocated of host disk. And Virtual machine analyser are typical in nature. So vmdk is same as computer system with the use of that we can directly access the user data of virtual machine but openly there is not any method or tool available for this file type which give a deleted data. However, in the list of total discovered files, forensic analyst must manually check the presence of these files. As the limitation of the virtual machine storage capacity we can not retrieve a data which previously deleted we only get recent deleted data because of overwriting of memory in the disk. In this paper we are try to get that virtual machine file recover and a method to open that file from that we can get the some part of deleted data files. In VMware it's very important to get access of vmdk file. Our future research goal on open a vmdk file in a user readable form with involve the deleted data caving techniques in default.

REFERENCES

[1] Juan Carlos Flores Cruz, Travis Atkison Louisiana Tech University Ruston,LA 71272 Digital Forensics on a Virtual Machine
[2] Hammad Riaz, Mohammad Ashraf Tahir 6th International Symposium on Digital Forensic and Security (ISDFS 2018)Analysis of VMware Virtual Machine in Forensics and Anti Forensics Paradigm
[3] https://pubs.vmware.com/workstation-10/topic/com.vmware.ws.using.doc/GUID-A968EF50-BA25-450A-9D1F-F8A9DEE640E7.html
[4] Vmware Technical Note, "Virtual Disk Format 5.0," Copyright © 2011 VMware, Inc. www.vmware.com
[5] Deleted VMware VMDK file information https://dtidatarecovery.com/deletedvmware-vmdk-what-should-you-do/
[6] https://www.cgsecurity.org/wiki/TestDisk



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY