Digital Forensics on a Virtual Machine

Juan Carlos Flores Cruz
Louisiana Tech University
Ruston, LA 71272
jcf028@latech.edu

Travis Atkison
Louisiana Tech University
Ruston, LA 71272
atkison@latech.edu

ABSTRACT

Hardware virtualization is a method that enables multiple isolated virtual machines (guests) to co-exist on a single physical computer (host). These virtual machines, which are created by a hypervisor, have a virtual environment that simulates its own set of hardware (CPU, hard disk, memory, network controller, and other components) and its own software [1]. Although virtualization is an old concept, it has become very important for IT infrastructures because it reduces hardware, management and energy costs. It does this by consolidating hardware and increasing server utilization. Virtual machines can be used for testing software, running different operating systems at the same time on a host, performing malware analysis, doing computer network simulation or service distribution, etc. As with any rapidly growing technology, there will be those that will use it for criminal activity. Because of this, a growth in our ability to accurately and efficiently perform digital forensics on a virtual machine environment must be addressed. Although virtual machines have been used as some of the tools to perform forensic investigations of criminal activities in physical machines, this does not provide the answer of what happens if the offender is performing its criminal acts in a virtual environment of a virtual machine instead of a physical machine. The principal objective of this paper is to explore some of the methodologies and techniques for performing forensics acquisition, authentication and analysis of a virtual machine; likewise, this paper will introduce some core methods that can lead to a good forensic analysis.

1. Introduction

Virtualization technology has developed rapidly because of the rapid decrease in hardware cost and concurrent increase in hardware computing power [2]. Consolidation, hardware and maintenance costs are some of the reasons for using virtual machines for enterprises. Companies can use a single server for multiple tasks that normally can take several physical servers to do them. Many companies have made extensive usage of virtualization to "virtualize" even entire networks to reduce costs and increase service efficiency. Distributed computing infrastructures are becoming increasingly virtualized, a principal purpose being to make it possible to safely share them across multiple applications, services, or even different application components. [3]

Although virtualization has helped IT infrastructures to reduce costs, it has brought new challenges for forensic investigators. Forensic investigations on virtual machines can become difficult to perform because their procedures might not be as effective as they are on physical machines. The offender can create a virtual machine to perform illegal acts in it and then delete all his/her traces by deleting the virtual machine. Likewise, he could uninstall the virtual application to make it more difficult for an investigator to know whether a virtual application was used in the physical computer in the first place or not.

Companies such as Microsoft, VMware, Oracle, Citrix are some of the companies that have created commercial and open source applications that many companies have adopted into their IT- infrastructures to create and deploy virtual machines throughout their networks. Because of the widespread use of these applications, making use of them has become easier and cheaper. Therefore, developing new methodologies and techniques to perform forensic investigations on virtual machines is crucial.

In this paper, we explore some tools and methods to perform digital forensics on virtual machines. Likewise, this paper will introduce some of the problems that are encountered when a forensic investigation has to be done on a virtualized environment. Although this paper will focus on VirtualBox, VMware Workstation and Microsoft Windows OS, the concepts and theories can be applied to other operating systems and virtual applications such as VMware Workstation/Sever/Player, Virtual-PC and Hyper-V.

2. Background and Motivation

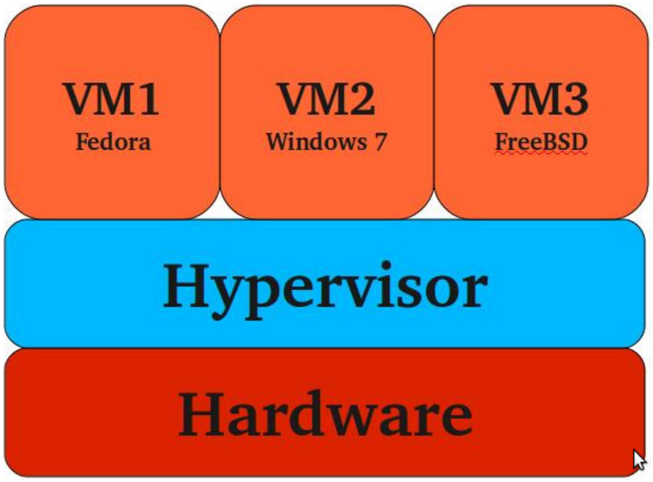
Virtual machines are becoming very important for enterprises because of the advantages they get from the technology. Nevertheless, this technology can be used for criminal activities, which makes forensic investigations more difficult to perform because of the complexity of this technology. There are many applications available on the internet that can be used by offenders to create and make use of these virtual machines for their activities. Computer forensics methodologies and techniques have to evolve to become effective on illicit activities on this new technology.

2.1 Hypervisors

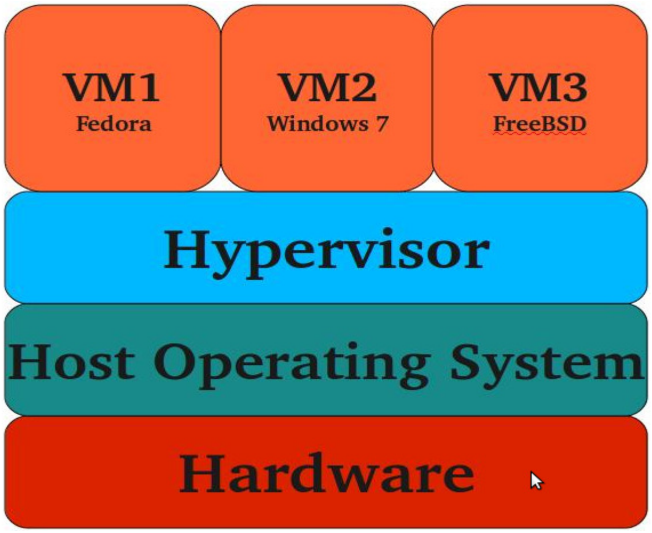
A Hypervisor or Virtual Machine Monitor is used to create and manage a virtual computer in a host machine. It is typically a small operating system that does not include hardware drivers. It is responsible for the hardware virtualization and execution of VM on top of the virtualized hardware. [5] The virtual machine presents the appearance of hardware to those processes that run on it including the resident operating system. [10]

The hypervisor allocates what each independent virtual machine requires at any given time by intercepting and simulating all the operating system operations in the virtual machine. It dynamically partitions and shares the hardware resources such as CPU, memory and I/O devices. [11]

Current virtualization methods exploit a combination of hardware (i.e., Intel VTD, AMD Pacifica) and software mechanisms, such as binary rewriting and para-virtualization. [4] Hypervisors are classified in two types of virtualization technologies, type-II and type-I. A type-I virtualization has direct access to resources, which makes its performance comparable to that of native execution. In contrast, type-II virtualization incurs additional overhead due to the layering of the VMM on top of the host OS when servicing resource requests from VMs. [5]



Type-1 Hypervisor Model



Type-II Hypervisor Model

Microsoft's Hyper-V, Xen, VMware ESXi are some examples of type-I hypervisors that are widely used. On the other hand hypervisors such as VMware Workstation/Server/Player, Virtual PC and VirtualBox are some examples of type-II hypervisors widely used on host operating systems. VirtualBox is an open source type-2 hypervisor that was originally created by software company innotek GmbH, which later was bought by Sun Microsystems, and now developed by Oracle Corporation. On the other hand, VMware Workstation, which is also a type-2 hypervisor, is a commercial hypervisor created by software company VMware, which is a division of EMC Corporation. These two applications are very common and easy to use because of their graphical user interfaces and extensive documentation. Although they have similar features, each one of them are good for certain

2.2 Computer Forensics

Computer forensics is the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on computer media [9]. Although there are many techniques and methodologies to perform forensic investigation on physical machines, very few have been developed to perform forensic investigation on virtual machines. Some of the basic forensic methods were to get the target disk without making any changes or damages to it, analyze the disk and to checksum all the data before and after the disk have been analyzed.

Virtualization has brought a new challenge for forensic investigators because they have to analyze systems that by nature are virtualized and isolated from host computer. Environment isolation and software compatibility are some of the features that forensic investigators can use to their advantage to analyze a physical machine image; however, these same features can be used by offenders to perform illegal activities.

3. Digital Forensic Method

In order to perform a forensic investigation on a host machine to recognize, acquire and analyze a virtual machine, we present 4 main steps. In this paper, we present how these steps can be applied to investigate a virtual machine for criminal activity. Describing every tool that is mentioned in this paper is not the objective of this paper; however, their purpose is important to mention for future reference.

- Forensic image creation
- Sensitive information identification and recovery
- Virtual machine analysis
- Documentation

3.1 Forensic Image Creation

The image creation process must always ensure that the data has not been modified and that the image is complete. Although this is a basic procedure when performing forensic investigations on a physical machine and has been described in many books and websites **[put references here]**, this is an essential procedure for the investigation of a virtual machine as well. The investigator should never use the original data to perform his investigation; therefore, it is important to create an image of the original data so that the investigator can use it for the analysis without modifying the original disk. Making a copy of virtual machine file(s) only is not desirable in an investigation because important files could be left behind and a complete investigation could not be possible without this information. Moreover, this information can help the investigator to gather more information about the virtual machine or hypervisor that was used. Execution time logs, temporary files, snapshots locations, Internet activity logs, etc. are some examples of the evidence that can be collected from the host machine if it is analyzed carefully. Valuable data related to the virtual machine may be of vital importance for the investigation; therefore, the investigator must capture the host media entirely.

Before an image is created, a hardware write-blocker must be used. Any modifications to the real disk can be detrimental for the investigation; therefore, using a write-blocker is essential to ensure no modifications will be made to the original disk. Likewise, system checksums must be taken to ensure that no data have been modified after the investigation has been completed. Forensic tools such as EnCase and X-Ways Forensics are some of the many available commercial tools to clone a disk or create an image of a physical disk as well as a virtual machine. Linux live CDs distributions such as CAINE and Backtrack can be used to clone or create an image of a disk as well. Likewise, they come with a large collection of open source forensic tools that can be used for the investigation. These types of forensic Linux distributions come with tools that can be used to create raw images of a disk. These images can be mounted on a different system to analyze it or extract the virtual machine to analyze it. Graphical user interfaces such has AIR and GuyMager, have been developed for tools such as dd and dcfldd, which makes them easier to use for investigator and users.

Below are some of the main steps that we recommend to follow to create an image

1. Obtain a hardware write-blocker read data from the original disk.
2. Checksum the original disk to ensure no changes have been done to the original disk after the investigation has been completed.
3. Boot up from a Live CD Linux Distribution to create an image or clone of the original disk to a different disk. Commercial application such as Encase or X-Ways Forensics can be used as well to create an image or clone of the original disk from in a different system.
4. Create necessary backups for data redundancy.
5. Store original disk in a safe place

During an investigation, the original disk should never be used to perform a forensic analysis. It should only be used for reference to all the forensic findings. Research in new approaches to use 2 different environments to perform forensics has been proposed. [1] In this research, two environments, conventional and virtual, are used independently to perform a forensic investigation. The original disk is analyzed by an investigator with greater experience in a conventional way; however, the created images are used by a less experienced investigator in a virtual environment without any write permission limitations. The less experienced investigator can report all his findings to the investigator with greater experience to validate the findings with the original data. This process can be efficient to analyze data from disk images without altering or limitation the forensic procedures to extract data from the disk

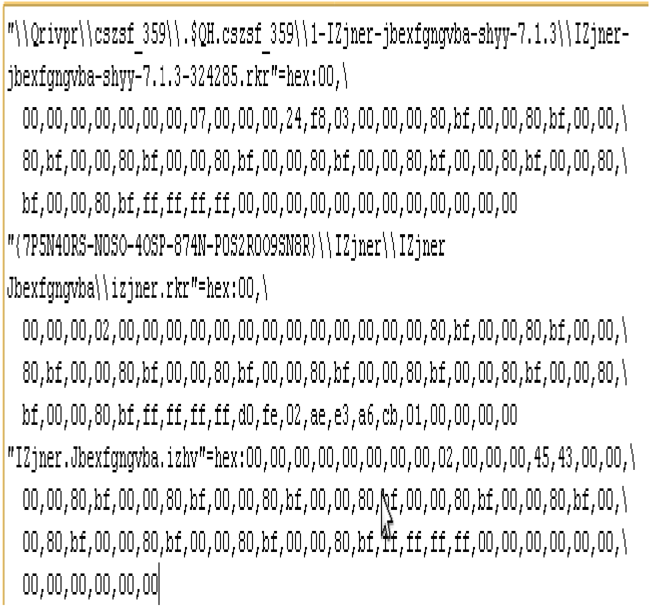
3.2 Sensitive Information Identification and Recovery

Before a forensic investigation on a virtual machine can be performed, it has to be found. An investigator has to find out whether an illegal activity was done from the host machine or from a virtual machine. Hypervisors are as any other application on an operating system. It can be uninstalled, corrupted or even improperly deleted. Many times the hypervisor will be installed in the host machine as well as the virtual machine, which makes it easier for the investigator to come to a conclusion for the type of system that was used; however, an offender could destroy all obvious evidence before the host machine is analyzed. This makes it more difficult for an investigator to detect whether a virtual machine has been used in the host machine or not. Therefore, proper analysis of the host has to be performed. Although finding traces of such application of virtual machine might not reveal all illegal activities done on the machine, they might give sensitive information to the investigator to continue his investigation. Likewise, all information can be crucial for other investigations and further analysis.

Having a good understanding of the host operating system is essential for any investigator because it allows him to find sensitive information about the suspect and his/her activities on the host machine. Operating systems can create keep logs of what users have done on a computer for debugging, management and record purposes. Analyzing this information can be tremendously helpful to the investigator to recover traces of a virtual machine or other illegal activities. Windows OS, for instance, creates registry entries, links, prefetch files, shared dlls, program icons, logs, thumbnails, temp data, system events, etc. for applications that have been installed or executed. By collecting and analyzing this data, the investigator can prove that a virtual machine existed in the host computer. Looking at file associations located in the registry can reveal information about applications that were installed in the host computer to open certain type of files such as .vmx, .vmdk, .vbox, etc, which are file extensions that belong to VirtualBox and VMware. Even if the user uninstalled the hypervisor, these file association would still point to them

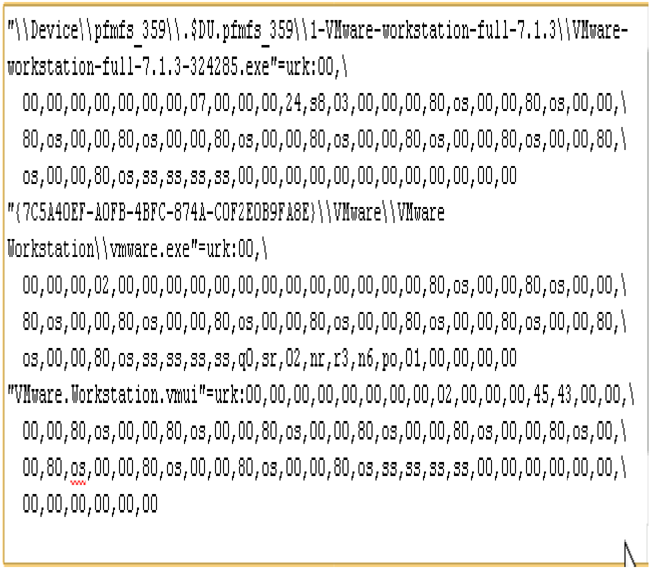
Figure 3.2.1 and Figure 3.2.2 are snapshots that we took to some registry entries that are created every time a piece of software is open in a Windows OS. The registry entries are encrypted with the ROT13 cipher, by extracting these entries from the windows registry and decrypting them we can reveal information that proves VMware and VirtualBox were open in the host machine. These registry entries are kept even when the application has been uninstalled.

Figure 3.2.1. Encrypted String



```
"\\Qrivpr\\cszsf_359\\.$QH.cszsf_359\\1-IZjner-jbexfgngvba-shyy-7.1.3\\IZjner-
jbexfgngvba-shyy-7.1.3-324285.rkr"=hex:00,\
  00,00,00,00,00,00,00,07,00,00,00,24,f8,03,00,00,00,80,bf,00,00,80,bf,00,00,\
  80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,\
  bf,00,00,80,bf,ff,ff,ff,ff,00,00,00,00,00,00,00,00,00,00,00,00
"{7P5N4ORS-NOSO-4OSP-874N-POS2ROO9SN8R}\\IZjner\\IZjner
Jbexfgngvba\\izjner.rkr"=hex:00,\
  00,00,00,02,00,00,00,00,00,00,00,00,00,00,00,00,00,80,bf,00,00,80,bf,00,00,\
  80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,\
  bf,00,00,80,bf,ff,ff,ff,ff,d0,fe,02,ae,e3,a6,cb,01,00,00,00,00
"IZjner.Jbexfgngvba.izhv"=hex:00,00,00,00,00,00,00,00,02,00,00,00,45,43,00,00,\
  00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,00,\
  00,80,bf,00,00,80,bf,00,00,80,bf,00,00,80,bf,ff,ff,ff,ff,00,00,00,00,00,00,\
  00,00,00,00,00,00
```

Figure 3.2.2. Decrypted String



```
"\\Device\\pfmfs_359\\.$DU.pfmfs_359\\1-VMware-workstation-full-7.1.3\\VMware-
workstation-full-7.1.3-324285.exe"=urk:00,\
  00,00,00,00,00,00,00,07,00,00,00,24,s8,03,00,00,00,80,os,00,00,80,os,00,00,\
  80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,\
  os,00,00,80,os,ss,ss,ss,ss,00,00,00,00,00,00,00,00,00,00,00,00
"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\VMware\\VMware
Workstation\\vmware.exe"=urk:00,\
  00,00,00,02,00,00,00,00,00,00,00,00,00,00,00,00,00,80,os,00,00,80,os,00,00,\
  80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,\
  os,00,00,80,os,ss,ss,ss,ss,q0,sr,02,nr,r3,n6,po,01,00,00,00,00
"VMware.Workstation.vmui"=urk:00,00,00,00,00,00,00,00,02,00,00,00,45,43,00,00,\
  00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,00,\
  00,80,os,00,00,80,os,00,00,80,os,00,00,80,os,ss,ss,ss,ss,00,00,00,00,00,00,\
  00,00,00,00,00,00
```

This is just one location of many in which Windows save files or logs that belong to executed applications or previously installed applications. This data must not be overlooked because it can be crucial for the investigation.

Files can get corrupted or deleted before an investigation can be performed. However, they can be fixed and recovered under certain circumstances. Deleted files can sometimes be recovered from temporary locations such has the Windows recycle bin or trash in a Mac, which are basically holding areas for deleted files. Depending on the virtual operating system, most virtual machine files are big, so operating systems do not move them to a temporary location because they would occupy a lot of storage space. Most operating systems do not overwrite the blocks on the hard disk that the file was written on when a file is deleted from the file system that the OS is using. Instead, they simply remove the file's reference from the containing directory. [7] In Windows systems, when a file is "deleted" its data link is actually removed from the Master File Table and marked as "overwritable"; however, the file itself can be recovered by using third party applications under certain circumstances. These third-party applications can be used to recover files even after they have been overwritten several times.

Files such as deleted snapshots, virtual machine configuration files and virtual hard drive files could be recovered by analysis the disk for deleted data. Recovering these files is essential for the investigation. Applications such as UNDELETE, Handy Recovery, R-Studio, Photorec/Testdisk are some of the many applications that can be used to recovered delete information from a disk. Once the files have been recovered the investigator can analyze them and use them to continue with the investigations. Although file recovery is possible with the right tools, they are some limitations to that can make file recovery almost impossible.

File encryption

Performing a forensic investigation on an encrypted can be difficult for an investigator because the data cannot be decrypted without the right key. Recovering an encryption key could be possible by performing a cold boot attack on a physical machine to recover the encryption key before it disappears from memory after the machine has been turned off [6]; nevertheless, this can become difficult to do because investigation could be made days or even months after the original disk have been recovered.

Physical destruction

In order to cover and hide all evidence, an offender can destroy the disk before it is recovered to be analyzed by an investigator. The offender could burn it or shred it to make an investigation on the disk impossible. Causing physical damage on the disk can be detrimental for the investigation because conventional tools could not be used to recover data from the disk. Although the act of destroying the disk could be used against the offender, it might not be enough prosecute the offender.

Degaussing

The offender could degauss its hard drive by exposing it to a powerful and alternating magnetic field to remove all previously written data. Degaussing the drive to randomize the magnetic domains will most likely render the hard drive unusable in the process. [7] An examination on the disk would be useless because conventional tools might not be able to recover any useful information.

Gutmann method

An offender could use use anti-forensic tools that use Gutmann's method and make data difficult or impossible to recover. Gutmann's method is a way to overwrite data many times with alternating patterns in order to expose the data to a magnetic field that oscillates fast enough that it flips the magnetic domains in a reasonable amount of time [8]. Open source, commercial and free tools have been written that use Gutmann's method ot similar methods. These tools can help an offender to delete sensitive data on a disk and make its retrieval difficult to perform.

Forensic investigation can become difficult to perform because of these limitations. Nevertheless, when the data cannot be recovered, the investigator must look for new alternatives to continue with the investigation. . It might be impossible to examine the virtual machine if the original disk has been destroyed or sanitized. Nevertheless, data backups, Internet activity logs, removable media analysis are some information alternatives that must be examined to continue with the investigation and to gather as much information as possible about the suspect. Although, they might not reveal as much information as the actual virtual machine, they could help to discover new clues such as passwords or information for remote backup locations that can be located before they are destroyed.

Although file corruption is not as common as it used to be, it can happen. Bad sectors, lost clusters, directory errors, etc can be some of the causes for file corruption; however, some disk tools could be used to fix these problems. Some operating systems such as Windows and Linux have tools that can be used to recover or fix corrupted files. If the virtual machine files have been recovered successfully the investigator can start performing an analysis on the images.

3.3 Virtual Machine Analysis

Depending on the investigation, analyzing the virtual machine can be very time consuming. The virtual machine can be analyzed by mounting it as a hard drive in a different machine or by using it with a hypervisor to get access to the virtual environment. There are many different hypervisors with their own proprietary file formats; hence, identifying the right format is very important for the investigation. Snapshots can contain sensitive information that can help for the investigation, thus they must be extracted and analyzed to see what changed have been made from the snapshot to the original virtual machine. Snapshots can provide useful information to the investigator about time and dates for files that were created or open when they were used with a virtual machine.

In order to analyze the virtual machine, the investigator has to get access to it. VirtualBox, for instance, supports Virtual PC and VMware image formats. By using VirtualBox an investigator can get access to the virtual environment of the virtual machine disk, even if, the virtual machine format is different. Similarly, Liveview, which is a java application, can create a VMware virtual machine out of a raw disk image or physical disk. By doing this, the investigator can analyze the content of the image. Other applications such as SmartMount and Mount Image Pro can be used to mount images to a system to analyze the content of the image. Most hypervisors come with a feature to take snapshots. This can be useful for an investigator to have different investigation stages during the virtual machine investigation as well as to compare results with different forensic tools when they are used on the same data and same virtual machine state.

Although the virtual operating system might have a password protection for the user account, the investigator can boot a live CD Linux distribution ISO image such as Backtrack or Ubuntu through the hypervisor to get access to the virtual machine content and change the password to get access to the virtual operating system environment. Chntpw, for instance, can be used to remove or change the password for a user account that is a member of a Windows OS. This is one of the many available password recovery tools that can be used to change or remove an user password.

As previously mentioned, the investigation must not be performed on the original data. An image of the data must be used. When the virtual machine file(s) are extracted from the created image, it must be analyze with the right tools. Once the investigator gets access to the virtual environment he can make use of many forensic tools that work for physical systems. A virtual machine environment is very similar to a physical machine environment. Thus, software that works in a physical machine has a great possibility to work in a virtual environment as long as the software is compatible with the virtual operating system. The tools depend on what the investigator is trying to investigate. File search, metadata extractors, file recovery, password recovery, log recovery tools are some of the many tools that can be used by an investigator to extract specific information from files that must be analyzed. Commercial forensic tools such as Encase, FTK and X-Ways Forensics can also be used to analyze and extract data from certain files such as email files, videos and pictures. Similarly, open source tools such as Autopsy (GUI for the Sleuth Kit) can also be used for a forensic examination. The scenarios can be many and it depends on what the investigator is trying to analyzed.

3.4 Documentation

Documentation about what has been found is crucial for the investigation. Likewise, it is necessary because it helps for any other future investigation that needs to be performed on the same data. Keeping record of who accesses the data, what they do with it and when they accessed it is very important for the investigation because it can ensure that all the changes and finding are valid. If any changes had to be made for any reason to the original disk, they must be recorded to validate them to the authorities or all the people that are involved in the investigation. Other investigators might need to analyze the data; hence, any changes to data must be notified to them.

All activities related to examinations, transfer of evidence, storage must be documented and available for future investigations or reviews. Many forensic tools come with their own report forms that can be used for simple documentation. However, a more detailed documentation is desired for any investigation.

4. Conclusion

Although virtualization has helped IT infrastructures to reduce costs, it has brought new challenges for forensic investigators. As with any rapidly growing technology, there will be those that will use it for criminal activity. Because of this rapidly growing technology, forensic investigations can become more difficult to perform because offenders can make use of it to try to bypass traditional forensic investigations that have been used on physical machines. New techniques and methodologies are needed to perform proper analysis on virtual machines. Although traditional forensic techniques can work to analyze virtual machines, new techniques must be developed to keep up with current and future computer technologies and how offenders can make use of these technologies to their advantage.

Forensic image creation, sensitive information identification and recovery, virtual machine analysis, documentation are the main steps that are mentioned in this paper to perform an efficient forensic investigation on a host machine. Although there are limitations that can affect the result of the investigation, an investigator can get a fair amount of sensitive information by following them.

In order for an investigator to perform an investigation on a system, he must become familiar with the host system to extract as much information from it. Even though an investigator might not be able to recover a virtual machine because of what the offender has done to it, he can still analyze all information that he can extract from the hypervisor itself.

In this paper, the main steps of a general methodology were presented to explore how an investigator could identify, acquire and analyze a virtual machine. Although this methodology is not perfect and future work is needed, it shows what could be done when an analysis on a virtual machine is needed to be performed. Virtualization is a technology that is here to stay, so research is needed for better and proper forensic analyses.

5. Future Work

Future research in the area of file acquisition and recognition is needed. Although the method that was mentioned in this paper can be used to perform forensics on a host system and its virtual machine(s), work is needed on this method to overcome its limitations. We will do this by finding new ways to recover as much sensitive evidence and information from what the offender has done, even if, the virtual machine cannot be recovered. Work on live data acquisition and analysis will be done to prevent loss of potential valuable evidence such as encryption passwords and memory resident malware traces. This is important to us because it greatly increase the efficiency of an investigation. We will do this by developing new techniques to extract data from a virtual machine or host machine while the system is running. Although this is just the beginning for us, it is an important step for further research in the areas of virtualization and digital forensics.

6. References

[1] D. Bem and E. Huebner, Computer Forensics Analysis in a Virtual Environment, *International Journal of Digital Evidence*, vol. 6, no. 2, 2007

[2] Qian L., Chuliang W., Minglu L., Yuan Lu., An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds, *Security & Privacy, IEEE* , vol.8, no.6, pp.56-62, Nov.-Dec. 2010

[3] Gavrilovska, A., S. Kumar, Abstract High-Performance Hypervisor Architectures:Virtualization in HPC Systems. Proc. of HPCVirt 2007, Portugal, Mar 2007.

[4] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the Art of Virtualization. In SOSP 2003, 2003.

[5] Vallee, G., Naughton, T., Engelmann, C., Hong Ong; Scott, S.L. , "System-Level Virtualization for High Performance Computing," *Parallel, Distributed and Network-Based Processing, 2008. PDP 2008. 16th Euromicro Conference on* , vol., no., pp.636-643, 13-15 Feb. 2008

[6] Halderman, J., Schoen, S., Heninger, N., Clarkson, W., Lest We Remember: Cold Boot Attacks on Encryption Keys, USENIX Security Symposium, February, 2008.

[7] Garfinkel, S.L., Shelat, A. , Remembrance of data passed: a study of disk sanitization practices, *Security & Privacy, IEEE* , vol.1, no.1, pp. 17- 27, Jan.-Feb. 2003

[8] Gutmann P., Secure Deletion of Data from Magnetic and Solid-State Memory, *6th USENIX Security Symposium Proceedings*, San Jose, California, July 22-25, 1996

[9] Kruse II, W. G., & Heiser, J. G., Computer Forensics: Incident Response Essentials (1st ed.): Addison Wesley Professional (2002)

[10] Nance K., Hay, B., Bishop, M., Investigating the Implications of Virtual Machines Introspection for Digital Forensics. *International Conference on Availability, Reliability and Security*. 2009

[11] Chen W., Lu, H., Shen, Li, Wang, Z., Xiao, Nong, Chen, Dan,. A Novel Hardware Assisted Full Virrtualization Technique. 9th International Conference for Young Computer Scientists, 2008.

[12] Hai J., Xiaofei L., Song W., Zhiyuan S., Yingwei L., , ChinaV: Building Virtualized Computing System, *High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on* , vol., no., pp.21-35, 25-27 Sept. 2008

[13] Vaughan-Nichols, S.J., New Approach to Virtualization Is a Lightweight, *Computer* , vol.39, no.11, pp.12-14, Nov. 2006

[14] Zhang Y., Lin Y., Research on the Key Technology of Secure Computer Forensics, *Intelligent Information Technology and Security Informatics.* Third International Symposium on , vol., no., pp.649-652, 2-4 April 2010

[15] Hayes, D.R., Qureshi, S., Implications of Microsoft Vista operating system for computer forensics investigations, *Systems, Applications and Technology Conference, 2009.*

[16] VMware.(2010).VMware. http://www.vmware.com/products/

[17] Oracle Corporation. VirtualBox. http://www.virtualbox.org/

[18] Guidance Software. EnCase. httpp://www.guidancesoftware.com/

[19] X-Ways Software Technology AG. X-Ways Forensics. http://www.x-ways.net/forensics/

[20] Kumar, A., Gentili, E., others. Backtrack 4. http://www.backtrack-linux.org/

[21] Canonical Ltd. Ubuntu. http://www.ubuntu.com/

[22] CAINE. CAINE. http://www.caine-live.net/

[23] Clarisoft. Undelete. http://www.glarysoft.com/products/utilities/glary-undelete/

[24] SoftLogica. Handy Recovery. http://www.handyrecovery.com/

[25] R-tools Technology. R-studio. http://www.r-studio.com/

[26] Grenier, C., Photorec and TestDisk http://www.cgsecurity.org/wiki/PhotoRec