# Design of Tool for Digital Forensics in Virtual Environment

Shagufta Rajguru
Assistant Professor
Department of Computer Engineering,
F. C. R. I. T. Vashi, India.

Aayush Pathak
Student
Department of Computer Engineering,
F. C. R. I. T. Vashi, India.

Danish K. Chaus
Student
Department of Computer Engineering,
Fr. C. R. I. T, Vashi, India.

Akshay J. Boramani
Student
Department of Computer Engineering,
F. C. R. I. T, Vashi, India.

## ABSTRACT
Virtual Environment Forensics is the process of performing the digital forensics in virtual environment. In recent time, virtualization technology has become one of the most important and popular technologies for individuals and companies due to its many advantages like cost benefits for storage, processing and computing resources. New techniques and methods of cybercrimes against virtual environments are used by attackers. Thus there is a need for designing and developing new techniques and tools to investigate new type of cybercrimes.[1]

In this paper, the computer forensic investigations with respect to the vital role of virtual environments have been analysed. Vulnerabilities in a virtual environment and some existing forensic tools are studied. We propose design of a forensic tool to analyse the evidences left by an attacker. Further this tool will try to relate the evidences in a presentable form which can be readily used by law enforcement to lead to the final suspect.

## Keywords
Digital Forensics, VirtualBox, Virtualisation, Evidence, Law

## 1. INTRODUCTION
### 1.1 Digital Forensics
Digital forensics is the process of collecting, extracting and recovery of digital evidence as an admissible proof about committed crime that will present it in the court of law. [1] The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. [2]

### 1.2 A Digital Forensics Model:
For this project, a stripped down specific version of the forensics model is used which includes the following steps: [3]

#### *1.2.1 Identification*
Recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps.

#### *1.2.2 Collection*
Record the physical scene and duplicate digital evidence using standardized and accepted procedures.

#### *1.2.3 Analysis*
Determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

#### *1.2.4 Presentation/Reporting*
Summarize and provide explanation of conclusions. The audience will be able to understand the evidence data which has been acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis component. [2]

### 1.3 BACKGROUND:
The organization of the report is as follows. Section 2 discusses about the virtual environment used. The section 3 discusses about the problem statement and various modules of the project. Section 4 gives proposed design. Finally, section 5 presents conclusion.

## 2. VIRTUAL ENVIRONMENT
### 2.1 Virtualbox: [4]
Oracle VM VirtualBox (formerly Sun VirtualBox, Sun xVM VirtualBox and Innotek VirtualBox) is a free and open-source hypervisor for x86 computers from Oracle Corporation. Developed initially by Innotek GmbH, it was acquired by Sun Microsystems in 2008 which was in turn acquired by Oracle in 2010. VirtualBox has been selected as the virtualization environment.

### 2.2 Virtualbox Architecture: [5]
VirtualBox uses a layered architecture consisting of a set of kernel modules for running virtual machines, an API for managing the guests, and a set of user programs and services. At the core is the hypervisor, implemented as a ring 0 (privileged) kernel service. Figure 1 shows the relationships between all of these components. The kernel service consists of a device driver named vboxsrv, which is responsible for tasks such as allocating physical memory for the guest virtual machine, and several loadable hypervisor modules for things like saving and restoring the guest process context when a host interrupt occurs, turning control over to the guest OS to begin execution, and deciding when VT-x or AMD-V events need to be handled.

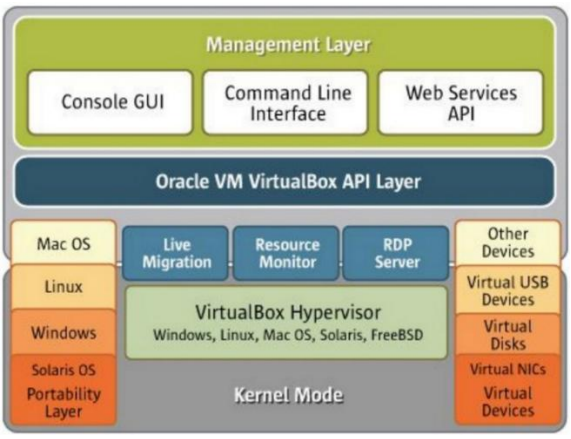


*Fig. 1: VirtualBox Architecture*

In addition to the kernel modules, several processes on the host are used to support running guests. All of these processes are started automatically when needed.

- *VBoxSVC* is the VirtualBox service process. It keeps track of all virtual machines that are running on the host. It is started automatically when the first guest boots.
- *vboxzoneacess* is a daemon unique to Solaris that allows the VirtualBox device to be accessed from an Oracle Solaris Container.
- *VBoxXPCOMIPCD* is the XPCOM process used on non-Windows hosts for interprocess communication between guests and the management applications. On Windows hosts, the native COM services are used.
- *VirtualBox* is the process that actually runs the guest virtual machine when started. One of these processes exists for every guest that is running on the host. If host resource limits are desired for the guest, this process enforces those controls.

# 3. PROBLEM STATEMENT AND PROJECT MODULES:

## 3.1 Problem Statement

To design a forensic tool to analyse the evidences left by an attacker. Further this tool will try to relate the evidences in a presentable form which can be readily used by law enforcement to lead to the final suspect.

## 3.2 Modules Of The Project:

### *3.2.1.1 Data deletion and modification:*

Data deletion consists of the files that were deleted after the clean snapshot and before the 2nd (dirty Snapshot). Similarly the new added files shall also be displayed.

Modified data shall include details of the files that were changed.

### *3.2.1.2 Modification of Virtual Machine Attributes:*

This module includes removal of Virtual Machine from the virtual environment (VirtualBox). [6]

### *3.2.1.3 Unauthorized Access:*

This module includes finding details of the unauthorized users who tried to access the system.

# 4. PROPOSED DESIGN [7][8]

The purpose of the project is to assist in detecting unauthorized intrusions by collecting and analyzing vital evidences left behind in a virtual environment. VirtualBox has been selected as the virtualization environment. The forensic tool will mainly explore malicious and doubtful activities conducted in the virtual system using VirtualBox such as:

- Data deletion and modification
- Modification of virtual machine attributes
- Unauthorized access.

This requires a thorough research for analyzing the technical background of VirtualBox and the host on which it is used. The proposed system will also depend on the guest operating systems that are used with VirtualBox. All of the above 3 activities leave traces in the form of files. Hence the proposed tool has to analyse both the files created by the virtual machine on the host machine and the files contained inside the virtual machines. There are two approaches of acquiring evidences from VMs:

a. To shut down and restart the suspected VM and scan inside it for evidence.

b. To take a live snapshot of the machine and analyse the files created by it on the host system.

The problem with the first approach is that while shutting down or restarting, a bunch of files and the volatile memory gets refreshed, which may result in loss of evidences and the analysis may not be presentable in the court of law. The second approach however, saves the current state of the VM which makes it dump all the data (including volatile) into files on the host system which can be later analysed. This is a clean and forensically sound way to scan for evidences without disturbing the VM in any way whatsoever.

To determine the files that have changed during the said criminal activity, we need a clean snapshot of the VM before the activity and a snapshot after it. Most enterprises take regular backups of their system including snapshots of VMs. Various hash functions can be used to compare the two snapshots and to generate a list of files that have been altered since the clean snapshot was taken. The tool will document the data in a presentable format. The results of the analysis can be of great use to law enforcement and courts to lead to the culprit. A generalized mechanism of the tool is as follows:

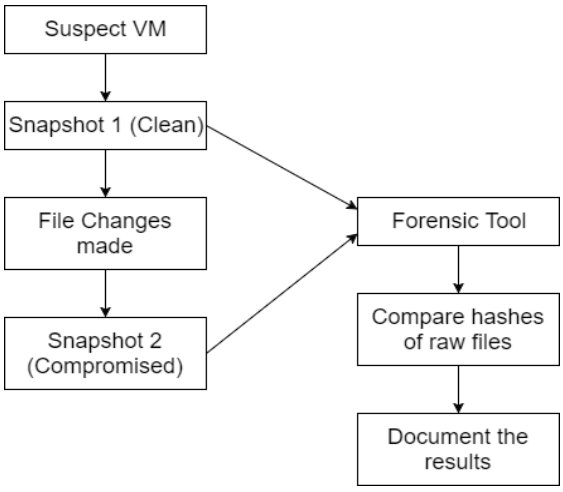


**Fig. 2: General Procedure of Forensics**

## 5. CONCLUSION

There are attackers who identify vulnerabilities in the virtual environment through different tools such as Nessus. These vulnerabilities can be used to violate the security and plan an attack on the system and gain unprivileged information. Then comes the role of forensic analyst who should have a thorough knowledge of working of the virtual environment and the storage of details in different log files. The forensic analyst should also be able to think from the attacker's point of view. [9] If the intentions of the attacker are known identifying the attacked location may be easier.

Therefore in this paper a proposed design of a forensic tool to analyse the evidences left by an attacker and document them to be used by law enforcement is given.

## 6. FUTURE SCOPE

As the future scope of this project we would like to implement the modules of the project. All the modules are independent from one another.

6.1 Data Deletion and modification.

6.2 Modification of Virtual Machine Attributes.

6.3 Unauthorized access.

The liability of the evidences should be checked. The chain of custody should be developed.

## 7. REFERENCES

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

[2] Shagufta Rajguru, Deepak Sharma "Database Tamper Detection and Analysis" International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 15, November 2014.

[3] International Journal of Digital Evidence - Fall 2002, Volume 1, Issue 3 http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

[4] https://en.wikipedia.org/wiki/VirtualBox

[5] Victor, Jeff, Jeff Savit, and Gary Combs. "Oracle Solaris 10 System Virtualization Essentials." InformIT: The Trusted Technology Source for IT Pros and Developers. N.p., n.d. Web. 31 July 2016.

[6] Cherilyn Neal "Forensic Recovery of Evidence from deleted Oracle VirtualBox Virtual Machines" Project Report, Utica College.

[7] https://blogs.oracle.com/fatbloke/entry/virtualbox_log_files

[8] http://searchvmware.techtarget.com/definition/VMware-snapshot

[9] Shweta Tripathi, Bandu Baburao Meshram "Digital Evidence for Database Tamper Detection" Journal of Information Security, 2012, 3, ***-*** Published Online April 2012 (http://www.SciRP.org/journal/jis)