International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(1): 63-71
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-0012

A Virtual Environment Forensic Tool

[#1]Danish K. Chaus,[#2]Aayush Pathak,[#3]Akshay J. Boramani,[#4]Shagufta Rajguru,[#5]Rakhi Kalantri

#1, #2, #3-Students
#4 and #5-Assistant Professor
Department of Computer Engineering,
F. C. R. I. T. Vashi, Navi-Mumbai,India.
danishkchaus@gmail.com,aayush.pathak15@gmail.com,
akshayboramani@gmail.com,shaguftai84@gmail.com
rakhi_kalantri@rediffmail.com

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 various cybercrimes.
We have analyzed the computer forensic investigations with respect to the vital role of virtual environments. Vulnerabilities in a virtual environment and some existing forensic tools are studied. In this paper, a forensic tool to analyze the evidences left by an attacker has been implemented. Further this tool documents the evidences in a presentable html form which can be readily used by law enforcement to lead to the final suspect.

KEYWORDS

Digital Forensics, evidence, law, VirtualBox, Virtualization.

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.

1.2 A Digital Forensics Model

For this project, we are using a stripped down specific version of the forensics model which includes the following steps as discussed below [4].

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 [3].

1.2.2 Collection

Record the physical scene and duplicate digital evidence using standardized and accepted procedures. Collection also involves finding the evidences from various sources of a particular system [3].

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 [3].

1.2.4 Reporting/Presentation

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 [3] [4].

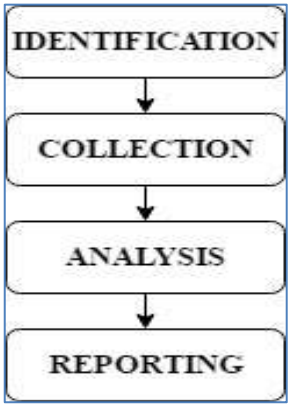

Fig.1: **Steps in Digital Forensics**

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 implementation details about various modules. Finally, section 5 presents conclusion. Section 6 highlights about the future scope that is yet to be implemented.

2 VIRTUAL ENVIRONMENT

2.1 Virtualbox

Oracle VM VirtualBox [5] (formerly Sun VirtualBox, Sun xVMVirtualBox and InnotekVirtualBox) 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 for the project.

2.2 Virtualbox Architecture

From fig.2 as mentioned below, Virtualbox uses a layered architecture [6] 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. 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.
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.

2.2.1 VBoxSVC

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.

2.2.2 Vboxzoneaccess

Vboxzoneaccess is a daemon unique to Solaris that allows the VirtualBox device to be accessed from an Oracle Solaris Container.

2.2.3 VBoxXPCOMIPCD

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.

2.2.4 VirtualBox

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.

2.3 Snapshots

A snapshot is a copy of the virtual machine's disk file (VMDK) at a given point in time. Snapshots provide a change log for the virtual disk and are used to restore a VM to a particular point in time when a failure or system error occurs [7] [8].

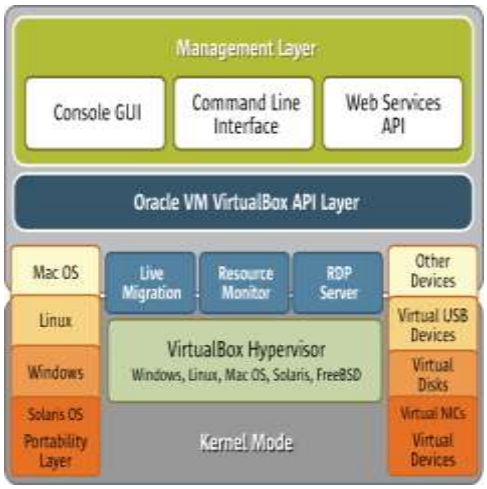

Fig.2: VirtualBox Architecture

3 PROBLEM STATEMENT AND PROJECT MODULES

3.1 Problem Statement

To design a forensic tool to analyze 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.
The tool analyzes data stored in files and volatile memory to scoop out potential evidences. The tool also uses hash functions to compare files with their consistent versions and will record the changes if any.

3.2 Modules Of The Project

3.2.1 Data Deletion and Modification

Data deletion consists of the files that were deleted after the clean snapshot and before the 2nddirty snapshot. Similarly the new added files shall also be displayed. Modified data shall include details of the files that were changed.
For the tool to work, we need a clean snapshot of the suspected VM i.e. a snapshot of the clean VM. We then collect another snapshot of the compromised VM. Both the snapshots are then run in the forensic tool. The tool uses a hashing algorithm to compare the two snapshots and as a result, return the files that have been changed since the clean snapshot was taken. These results are interpreted and documented.

3.2.2 Modification of Virtual Machine Attributes

This module includes removal of Virtual Machine from the virtual environment (VirtualBox).
EventViewer and EventLogs are logging tools within the VMs which contain information about authentication requests, root accesses etc. The VM_OS_Logs are log files generated by VirtualBox which contain the machine state and various parameters related to it. The forensic tool that is implemented in this paper can be used by the analyst to generate the report to be read by Law Enforcement if the parameters of the virtual machine are compromised.

3.2.3 Unauthorized Access

This module includes finding details of the unauthorized users who tried to access the system.
Using the log files the tool is able to read authentication logs and match the timestamps to find out under whose authentication, the changes were made. The tool will also list potential evidences and document them in an understandable format.

4 IMPLEMENTATION

Snapshot feature of VirtualBox has been used as an evidence in the project. Multiple Snapshots shall be taken at regular intervals. These Snapshots shall be merged to create a clean and a dirty machine. These 2 machines shall be compared to find the evidences and document them. The

following are the steps to create the VM's and Snapshots.

- Create a new Virtual Machine in the VirtualBox using Ubuntu 14.04 as Guest OS.
- Create the virtual hard drive as a fixed sized VDI file and stored it in the "C:\Users\Test\ VirtualBox VMs\Ubuntu 14.04" directory.
- This creates a folder named "UbuntuMain" in the Vbox VMs folder. All the details such as machine logs, snapshots, etc of the machine will be stored inside this folder.
- Take a clean Snapshot (Snapshot1).
- Make some changes in the VM i.e create/delete/modify some file or folder.
- Take another Snapshot (Snapshot2).

4.1 Data Deletion and Modification

The Digital Forensics process consists of steps such as:
1. Identification
2. Collection
3. Analysis
4. Reporting/Presentation

Evidence identification and collection process should be carried out at the Suspect Machine i.e. the machine at which the crime has occurred. Analysis of these evidences should not be done at the Suspect Machine as the evidence might get lost or modified. The Analysis needs to be done separately at the investigator's machine. Thus, we propose a separate Acquisition tool for collecting the evidence (snapshots) from the Suspect Machine.

4.1.1 The Acquisition Tool

The Acquisition tool shall be used at the suspect machine to acquire (collect) evidences. The Acquisition tool consists of 2 parts:

4.1.1.1 Clone Snapshots

A snapshot just stores the changes in a VM. Thus it cannot be directly used. Snapshot needs to be merged with a base before mounting it. This process is termed as Clone Snapshot. It creates 2 vmdk files:

- UbuntuMain-clean: A clean VM before any modification was made to the system.
- UbuntuMain-dirty: VM after some files in the system were modified / deleted.

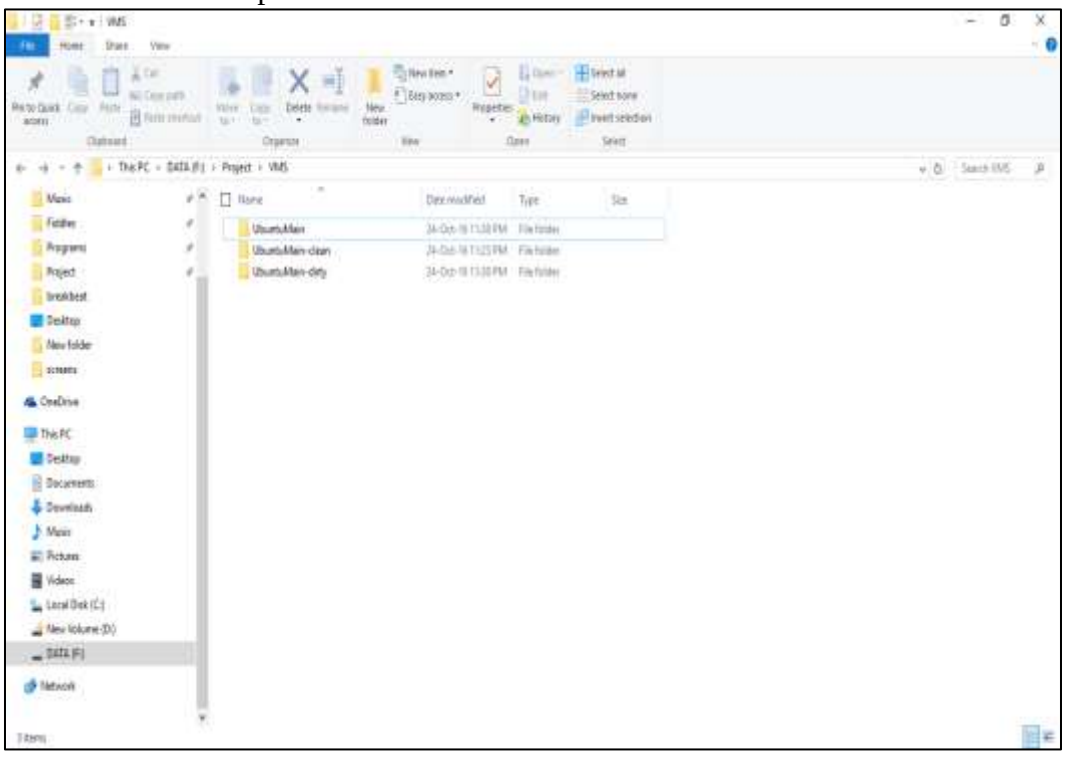

Fig.3: Folder structure of VMS after the 2 new VMs are created

4.1.1.2 Acquire Raw Image

The vmdk files cannot be directly opened to identify the changes. Thus they need to be converted to Raw images. The 2nd step of Acquisition Tool does this process of converting the two machines into two Raw images. This completes Identification and Collection process. These images are then transferred to the investigators machine for analysis.
The following is the procedure to convert Raw images to VDI/VMDK format using VirtualBox command-line interface (VBox Manage) [2]:
1. Suppose we have raw image of sdb device:
$ sudodd if=/dev/sdb of=./sdb.raw
2. Convert it to VDI format in order to use it with VirtualBox:
$ VBoxManageconvertddsdb.rawsdb.vdi --format VDI
3. Convert it to VMDK format in order to use it with VMWare:

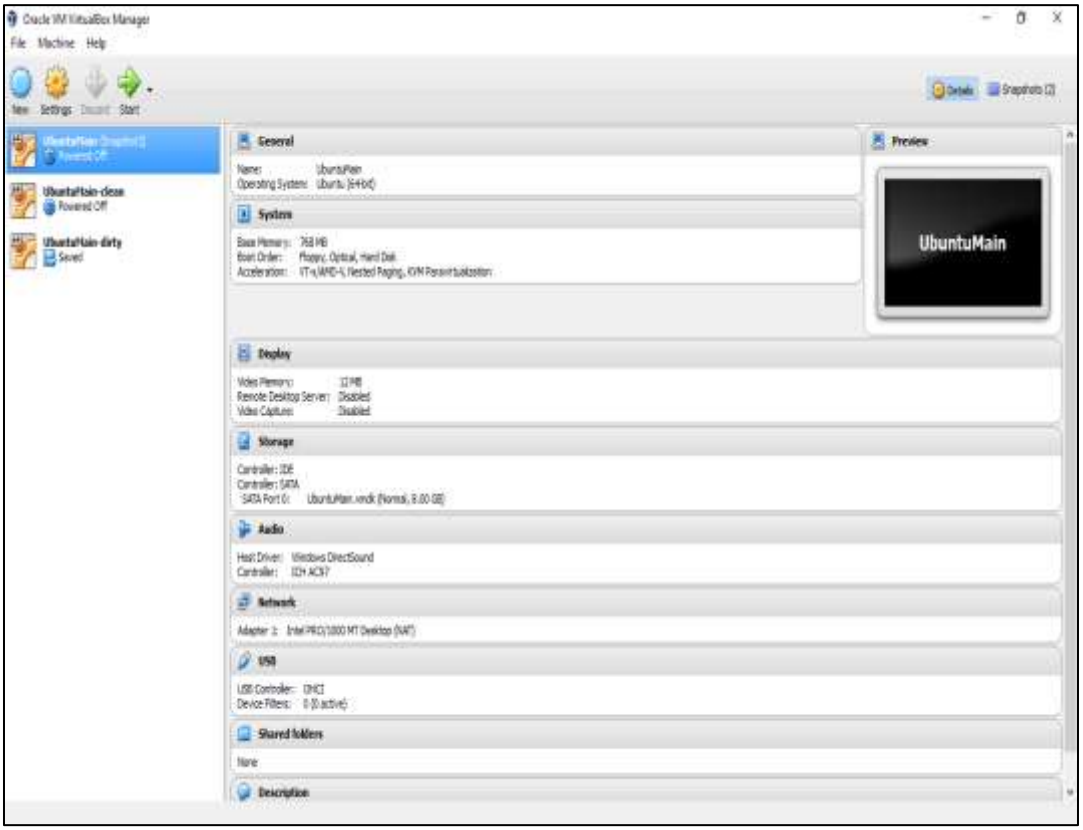

Fig.4: New VMs are created in the VirtualBox

$ VBoxManageconvertddsdb.rawsdb.vmdk --format VMDK
4. Convert between VDI/VMDK formats:
$ VBoxManageclonehdsdb.vdisdb.vmdk --format VMDK
$ VBoxManageclonehdsdb.vmdksdb.vdi --format VDI
5. Converting to raw image:
$ VBoxManageclonehdsdb.vdisdb.raw --format RAW

4.1.2 The Virtual Forensic Tool

Once the Raw images are created using the Acquisition tool, they are then transferred to the investigators machine for further Analysis.
In the fig.5 the block diagram for the acquisition

tool is given. Similarly, fig.6 shows the implemented results from the acquisition tool in the form of two raw images.

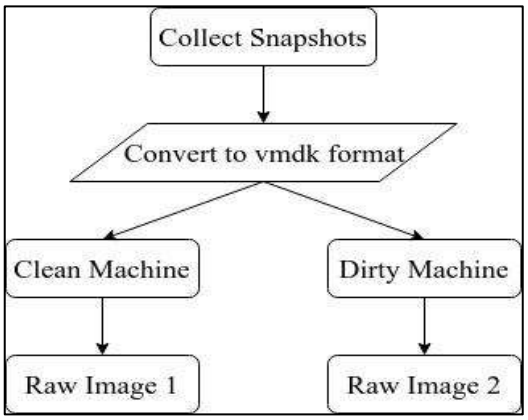

Fig.5: Working of Acquisition Tool

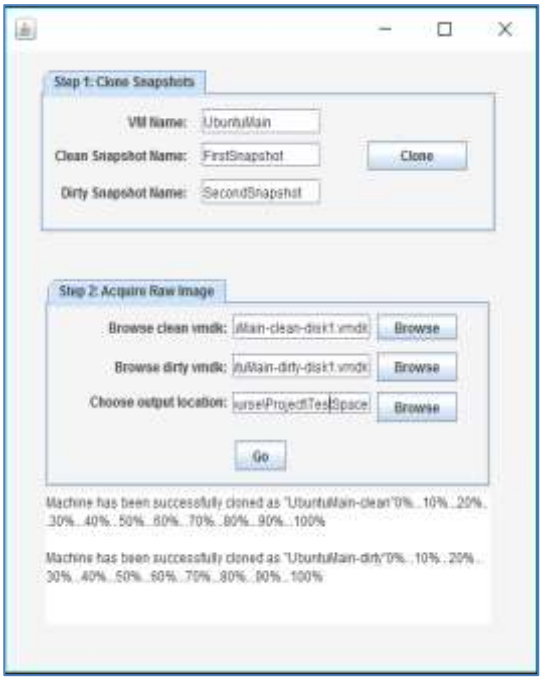

Fig.6: Acquisition Tool

The process at the investigator's machine is as follows:

4.1.2.1 Create New Case

The investigator shall create a new case by entering the details for the case. These details include Case Name, Date, Location to save details, description of case and Investigators Name. In the fig.7 given below a GUI for the investigator to register a new case has been implemented. A database of such new cases can be created and stored.

Fig.7: Virtual Forensic tool (create new case)

4.1.2.2 Select Files/Folders to compare

Investigator can now select any folder or file from the clean machine and compare it with the file or folder from the dirty machine. Hash is generated for comparing the files and thus results are displayed in the Results tab present at the top in figure 8. Here MD5 algorithm is used in order to generate the hash values. With the mismatch in the hash values it becomes clear that the file has been compromised.

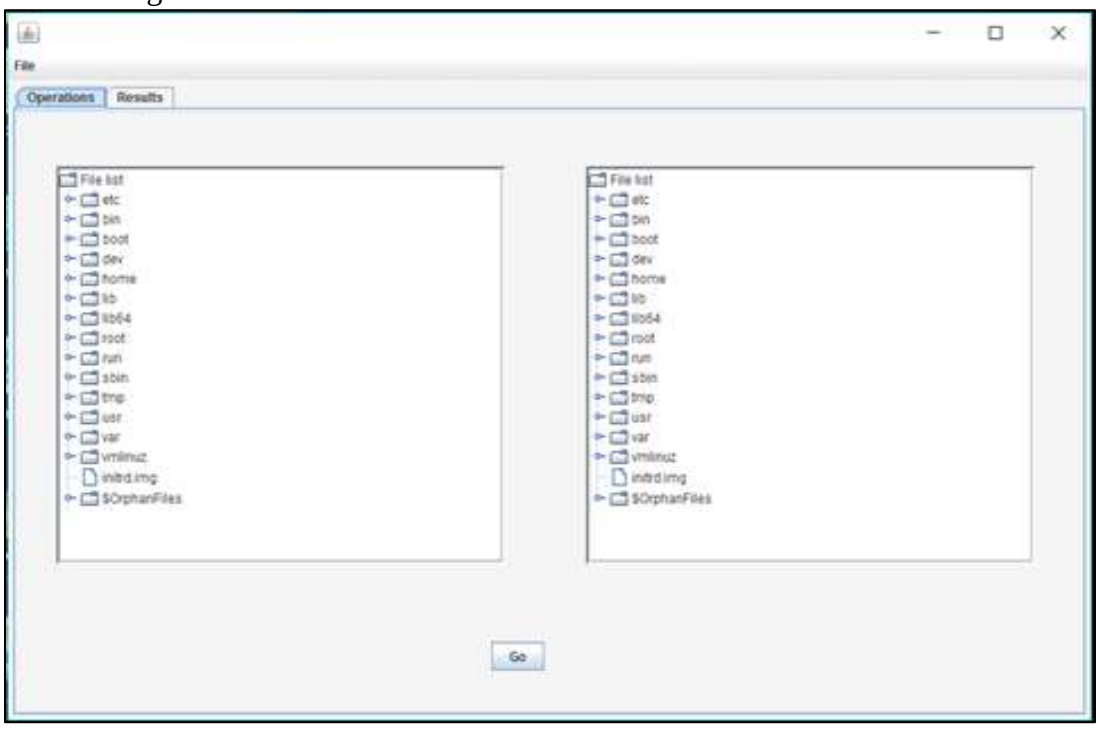

Fig.8: File tree for Clean and Dirty image

4.1.2.3 Display Results

The results in the fig.9 include the list of added or deleted files and the modified files. These results can be exported in an html format report. This report can be used by the law enforcement as an evidence to lead to the final suspect.

4.2 Modification of VM Attributes

Modification of VM Attributes includes Removal of a Virtual Machine from the VirtualBox Manager. It can be done by using the following steps:

Right Click on the VM --> Select 'Remove'.
In such a case, the evidence can be found in the VirtualBox log files. The VirtualBox log files are present at the following locations [9]:

- **Windows:**%HOMEDRIVE%%HOMEPATH%\\.VirtualBox\\Machines\\<vmname>\\Logs\\vbox.log
- **Mac:**$HOME/Library/VirtualBox/Machines/<vm name>/Logs
- **Linux:**$HOME/.VirtualBox/Machines/<vm name>/Logs

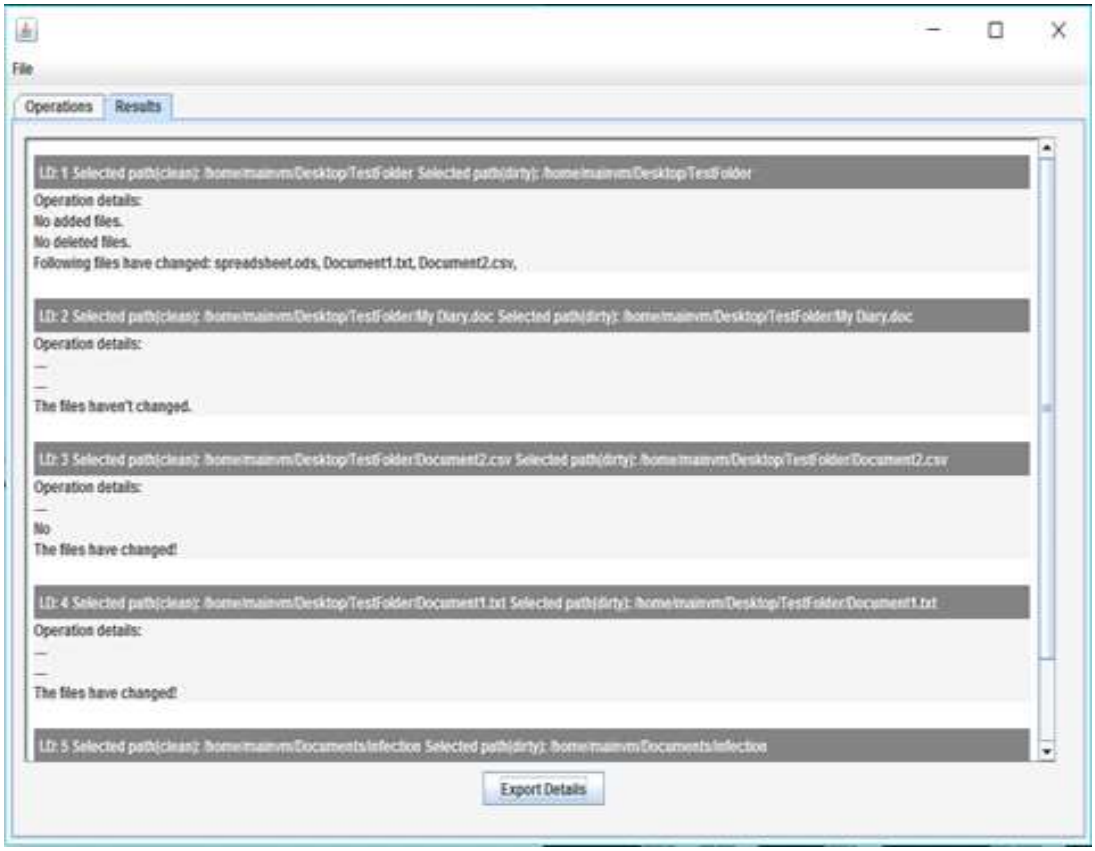

Fig.9: Results of operations

5 CONCLUSION

The attackers identify vulnerabilities in the virtual environment through different tools. These vulnerabilities can be used to violate the security and plan an attack on the system and gain sensitive information. The forensic analyst 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 [10] [11]. If the intentions of the attacker are known identifying the attacked location may be easier.
Therefore in this paper a forensic tool has been implemented that analyzes the evidences left by an attacker and document them to be used by law enforcement.

6 FUTURE SCOPE

As the future scope of this project we would like to implement the third module (Unauthorized Access) of the project. This module shall make use of "auth.log" file which gives the login details of different users of the system to check if the login was authorized or unauthorized.

REFERENCES

[1] Manjaiah D.H, Ezz El-Din Hemdan "Digital Forensics in Virtual Environment" CSI Magazine, March_2016.
[2] https://blog.sleeplessbeastie.eu/2012/04/29/virtualbox-convert-raw-image-to-vdi-and-otherwise/
[3] ShaguftaRajguru, Deepak Sharma "Database Tamper Detection and Analysis" International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 15, November 2014.
[4] International Journal of Digital Evidence - Fall 2002, Volume 1, Issue 3.
[5] https://en.wikipedia.org/wiki/VirtualBox
[6] 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.
[7] https://blogs.oracle.com/fatbloke/entry/virtualbox_log_files
[8] http://searchvmware.techtarget.com/definition/VMware-snapshot
[9] Cherilyn Neal "Forensic Recovery of Evidence from deleted Oracle VirtualBox Virtual Machines" Project Report,

Utica College.
[10] ShwetaTripathi, BanduBaburaoMeshram "Digital Evidence for Database Tamper Detection" Journal of Information Security, 2012, 3, ***-*** Published Online April 2012.
[11] ShaguftaRajguru, AayushPathak, Danish K. Chaus, Akshay J. Boramani "Design of Tool for Digital Forensics in Virtual Environment" International Journal of Computer Applications (0975 – 8887) Volume 163 – No.4,April-2017