Data preservation and digital forensics for virtual machines

MS Thesis

Adviser: Dr. Malik Tahir Hassan

Student: Taimour Nazar s2016114004

Department of Software Engineering

School of Systems and Technology

University of Management & Technology, Lahore, Pakistan

Reviewed By

1. Dean _____

   School of Systems and Technology

   UMT Lahore, Pakistan

2. Adviser _____

   School of Systems and Technology

   UMT Lahore, Pakistan

3. Director of Graduate Studies _____

   School of Systems and Technology

   UMT Lahore, Pakistan

ABSTRACT

Cloud computing is an emerging trend these days. It offers computation and storage at a relatively low-cost due to its pay per use policy. However, it has created new concerns regarding security, as all the conventional methodologies and tools for investigation fall short for cloud computing investigation. Study of recent research papers has shown that no definite strategy exists to cater this issue. Certain methodologies have been proposed by researchers but a major issue, i.e., loss of records which is vital for digital forensics due to termination of virtual machines, remains unsolved and unaddressed. Our main aim is to address this issue and propose a possible and practical solution for it. All terminating virtual machines cannot be stored for forensic because of high cost of storing huge amount of data. In our solution only relevant data of virtual machines will be stored as an XML file. Further a list of software is extracted from this XML file and it is used to find out how much risky is this virtual machine and it can give an idea to forensics experts that what type of malicious activity could have been conducted with it before it was terminated.

ACKNOWLEDGMENT

I am thankful to Almighty Allah. I am thankful to all my teachers and my parents for their prayers and support. I would like to acknowledge the help and support of my advisor Dr. Malik Tahir Hassan who provided guidance in completing this thesis.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction and Background

1.1 Forensics

Forensics uses some scientific techniques and tools to find details of a criminal act. Results of forensics techniques helps in proving or disproving a crime. Since long ago interpretation and observation were used as basic tools in forensic science [15]. Initial step is to observe the crime scene and collect all evidences found on the crime scene. During collecting of evidence, investigator collects evidence without thinking about the potential importance of the evidence. Which evidence is potentially important is decided later after reconstruction of the timeline [16].

In forensic sciences, there are seven S (Figure 1.1) of crime scene investigation [16] as following:

1. Securing the scene
2. Separating the witnesses
3. Scanning the scene
4. Seeing the scene
5. Sketching the scene
6. Searching for evidence
7. Securing and collecting evidence

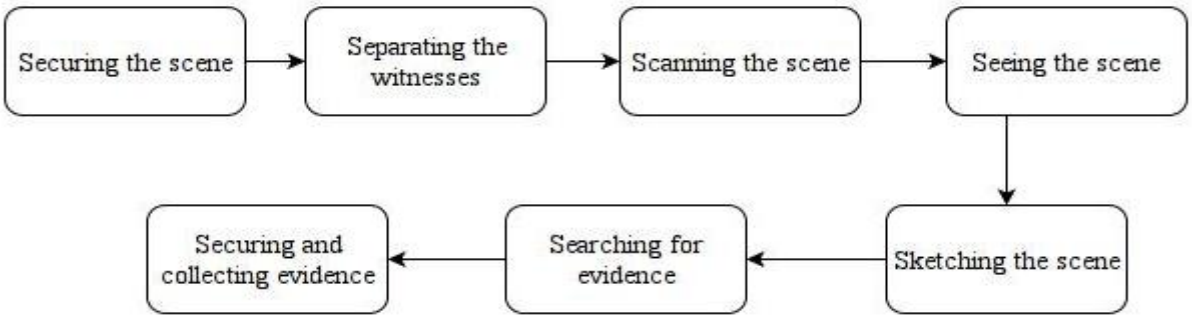

Figure 1.1: The seven S of crime investigation