

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

Reviewed By	2
ABSTRACT.....	3
ACKNOWLEDGMENT	4
Table of Contents	5
List of Tables	7
List of Figures	8
Chapter 1: Introduction and Background.....	9
1.1 Forensics	9
1.2 Digital Forensics	Error! Bookmark not defined.
1.3 Cloud Computing.....	Error! Bookmark not defined.
1.4 Cloud Computing and Digital Forensics.....	Error! Bookmark not defined.
1.5 Problem statement.....	Error! Bookmark not defined.
Chapter 2: Related work	Error! Bookmark not defined.
2.1 Related literature	Error! Bookmark not defined.
2.2 Related tools.....	Error! Bookmark not defined.
2.3 Related commands	Error! Bookmark not defined.
Chapter 3: Identified Major challenges and their solutions	Error! Bookmark not defined.
3.1 Challenges for digital forensics in a cloud computing environment	Error! Bookmark not defined.
Chapter 4: Methodology	Error! Bookmark not defined.
4.1 Proposed solution for data lost after termination of virtual machine.....	Error! Bookmark not defined.
4.2 Proposed structure for XML file.....	Error! Bookmark not defined.
4.3 Threat level detection from XML file.....	Error! Bookmark not defined.
4.4 Advantages.....	Error! Bookmark not defined.
4.5 Evaluation Methodology.....	Error! Bookmark not defined.
Chapter 5: Existing tools, categorization and their uses	Error! Bookmark not defined.
5.1 Tools for Information gathering.....	Error! Bookmark not defined.
5.2 Tools for analysis vulnerabilities present in target	Error! Bookmark not defined.
5.3 Tools for exploitation of target	Error! Bookmark not defined.
5.4 Tools for conducting forensics.....	Error! Bookmark not defined.
5.5 Tools to focus web applications.....	Error! Bookmark not defined.
5.6 Tools for stress testing	Error! Bookmark not defined.

5.7 Tools for sniffing and spoofing.....	Error! Bookmark not defined.
5.8 Tools for password attacks.....	Error! Bookmark not defined.
5.9 Tools for maintaining backdoor access.....	Error! Bookmark not defined.
5.10 Tools for reverse engineering	Error! Bookmark not defined.
5.11 Tools for reporting	Error! Bookmark not defined.
5.12 Advantages of categorization.....	Error! Bookmark not defined.
Chapter 6: Experimentation and result.....	Error! Bookmark not defined.
6.1 Experimentation	Error! Bookmark not defined.
6.2 Results.....	Error! Bookmark not defined.
Chapter 7: Summary	Error! Bookmark not defined.
References	Error! Bookmark not defined.

List of Tables

No	Tables	Page no
1.1	Service Models	11
1.2	Deployment Models	11
2.1	Linux commands for hardware and software details	19
4.1	Description of tags in proposed XML file	26
5.0	Categorization of tools	32
5.1	Information gathering tools	33
5.2	Vulnerability analysis tools	34
5.3	Target exploitation tools	35
5.4	Forensic tools	36
5.5	Web application tools	37
5.6	Stress testing tools	38
5.7	Sniffing and Spoofing tools	38
5.8	Password attack tools	39
5.9	Maintaining back door access tools	40
5.10	Reverse engineering tools	41
5.11	Reporting tools	41

List of Figures

No	Figures	Page no
1.1	The seven S of crime investigation	9
1.2	Steps for digital forensics	10
1.3	Five essential characteristics	11
1.4	Digital forensics in cloud computing	12
2.1	Hardinfo	15
2.2	I-Nex	16
2.3	Sysinfo	16
2.4	Hardware lister	17
2.5	KInfoCenter	17
2.6	Dmidecode	18
2.7	Hwinfo	18
3.1	Multi tenancy model	21
4.1	Creation of XML file before deletion of VM	24
4.2	Threat level detection from XML file	28
4.3	Steps for reconstruction and forensics of VM	29
6.1	AntiX detected tools bar graph	76
6.2	Kali detected tools bar graph	77
6.3	Deft detected tools bar graph	78

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

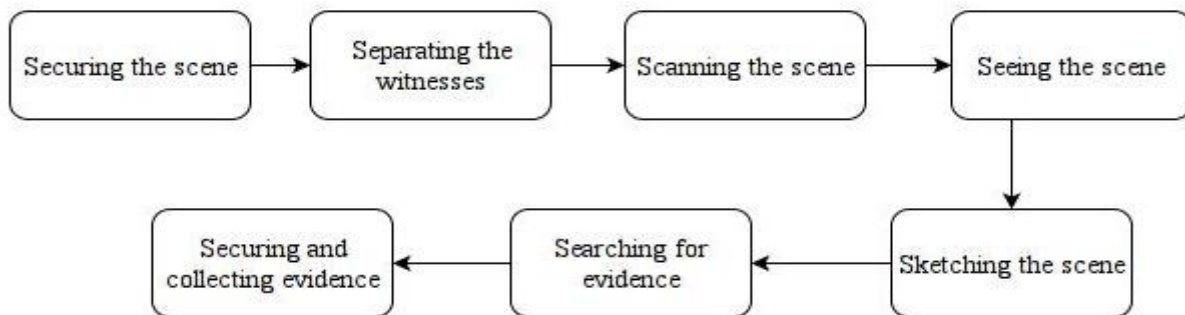


Figure 1.1: The seven S of crime investigation