GUI BASED MEMORY FORENSICS TOOLKIT FOR ANALYSIS AND EXTRACTION OF MALICIOUS PROCESSES

Vivek Ravindra Sali[1], Harmeet K. Khanuja[2]
[1]Department of Computer Engineering, MMCOE, Pune
[2]Assistant Professor, Department of Computer Engineering, MMCOE, Pune

Abstract
The success of the digital investigation is dependent on the availability and maintaining the quality of the data being collected. Because the digital evidence that is collected must be presented in its original form to the court for the proof against the crime. In this project one of the methods of digital forensic investigation is discussed which is memory imaging analysis.
The advantage of the investigation method used in this project offers the efficient and easy use of forensics tools that are based command line approach, by introducing them under common GUI framework. Memory forensics is one of the branches of the Computer Forensics. The present techniques of memory forensics like Live Response and Memory Imaging, used by investigators during analysis and seizure operations involves either carrying the live analysis of volatile memory(RAM) of victimized computer system or by making the image of the RAM of suspect's machine and performing post analysis on different machine. In this paper Memory imaging approach of RAM analysis is used to find out the malicious processes using the GUI based tool that can analyze the volatile memory artifacts those are affected by malwares. The architecture of extracting the malicious processes is mentioned in this paper.
Index Terms: Digital investigation, digital evidence, GUI framework, computer forensics, volatile memory dump, Live Response, YARA Scanner.

I. INTRODUCTION

The computing resources and Internet play a significant role as vital business tool to provide the necessary information to an individual. Due to massive use of the Internet, cybercrime has been increased. Cybercrime is any illegal activity which involves a computer system or it's related systems or their applications.
Today solving any cybercrime put up new challenges for a digital forensics investigator[5]. Digital forensics is the process of uncovering and interpreting an electronic data. The goal of investigation is to preserve the evidence that is obtained during an investigation process. This evidence is termed as digital evidence which must be preserved to reconstruct the past events. The analysis of volatile memory plays a very significant role in a process of digital investigation process. The volatile memory contains many important artifacts which can be used in forensic investigation process. The information may contain passwords, event logs, cryptographic keys, process information and other vital data related to number of processes running in a system[2][8].The collection of volatile data from a victimized computer system under investigation can be done using a conventional approach known as Live Response approach. In this approach the investigator first establishes a trusted command shell to acquire the data for investigation process. Volatile memory analysis using a Live Response method helps to collect all relevant evidences from a system. These evidences can be used to prove any incident occurred that might have compromised a system resulting into a cybercrime [2].
Another method to analyze a volatile memory is to perform memory image analysis. The analysis of a volatile memory is performed by capturing an image of RAM known as memory dump .Digital forensics contains the collection, validation, analysis, interpretation,

documentation and presentation of the digital evidences [15]. Digital Forensics investigator makes use of forensics tools in an investigation process, which are present in commercial and open domains. Depending upon the requirement of analysis, forensic toolkits are categorized like file system and data analysis tools, memory analysis tools, disk analysis tools, registry analysis tools, Internet analysis tools and many more analysis tools. The commonly used toolkits for analyzing file systems are Encase, FTK, X- Ways, Nuix, Sleuthkit, DFF, Snorkeland LibForensics. Of these tools, Encase, FTK and X-Ways are commercial toolkits while Sleuthkit, DFF and LibForensics are in open domain. To extract the malicious processes out of the genuine processes from memory image, the file signature scanner tool known as YARA tool can be used. The YARA is an open source tool designed to help malware researcher to identify and classify malware samples. Using YARA Scanner tool one can create description of malware families those are based on binary and text patterns. It uses the efficient pattern-matching rule.YARA supports the use of three different types of strings for pattern-matching:

(a) Hexadecimal Strings
(b)Text Strings based on ASCII text
Regular Expressions

Users can write their own set of rules for YARA Signature Scanner to find the malicious files, only condition is that the criteria for writing the rule must be necessary part of behavior of malware. Also, the criteria must contain something that is common across different samples.

II. REVIEW OF L ITERATURE

Timothy Vidas [1] discussed the benefits and drawbacks of traditional incidence response methods. RAM analysis using RAM duplicates provides least but similar information that incident response tools can provide. Even more information can be gained from RAM duplicate. RAM acquisition permits the user to analyze the contents after first response and it enables RAM data to be considered more precious and additional source as a static evidence item in digital forensics investigation process. Amer Aljaedi et al.[2] Proposed the comparison between two memory analysis approaches like Live Response and memory imaging. Memory imaging can be an alternative approach to retrieve and recover volatile data. Live response approach of memory analysis can be a troublesome as it can overwrite the potential evidences such as terminated and cached processes which will be ignored during this approach. In memory imaging analysis process the vital evidences like cached processes, some Internet artifacts can be extracted
directly from the memory dump. Memory image analysis tech- nique help in detecting the malware and anti-forensics methods. Robert J. McDown et al.[3] have presented the study of seven open source RAM acquisition forensic tools those are compatible to work on 64-bit windows operating system. The parameters like total execution time, platform limitations, reporting capabilities, shared and proprietary DLLs, modified registry keys and invoked files were compared in the study. Forensics tools like Windows Memory Reader and Belkasoft Live Ram Capturer leaves behind the least fingerprints, whereas ProDiscover and FTK Imager perform very poor as per memory usage, processing time, DLL usage and unwanted artifacts introduced in the system is concerned. Belkasoft's Live RAM Capturer is the fastest to obtain an image of the memory than ProDiscover tool takes the time to do the same task.

Sriram Raghvan et al.[4] presented the study of contemporary forensic and analysis tools based on different functionalities supported by these tools. Different capabilities of some tools are studied to examine one or more sources of digital evidence. The study highlighted the importance of metadata and its use across the heterogeneous sources of digital evidences.

Ala Berzinji [5] presented the cyber forensics methodologies of capturing, processing and investigating data from the computer system to discover the evidence that is acceptable in court of law. Forensic investigation tools like DumpIt, FTK Imager, Volatility Framework, Hashing tool are used to find out the evidences out of the system.

Ezer Osei Yeboah-Boateng et al.[6] Presented the study to reconstruct timeliness of activities on infected systems. Data from infected systems is collected using memory image and live response tools to analyze the payload. It is the best practice to make a memory image before beginning the analysis as original copy

can be kept safe while the duplicate copy can be analyzed. The compromised system under the investigation process is windows OS and while examining the memory image using Master File Table(MFT) attributes which includes the file name, time stamp as well as index entries.

Elick Chan et al.[7] designed a framework, ForenScope for a volatile state analysis that allows the investigator to explore and control the victimized computer system through interactive 'bash' shell. The ForenScope framework preserves the snapshot of memory to a flash drive like USB and installs a software write blocker to prevent alteration to the disk without violating the semantics of running program.

Amulya Podile et al.[8] discussed the analysis of various memory artifacts of volatile memory to identify the malwares. The analysis of system logs and registry from RAM Image of Windows Operating System was carried out using some open source and commercial forensic tools like Volatility, En-case etc. The authors confirmed the source of attack, time-stamp behavior of the malware.

R. Raines et al.[9] proposed the malware recognition via static heuristic methodology. The experiment was carried out on 32 bit Portable Executable(PE) files. Samples of file Strings were taken using the hex dump tool.

Christodorescu et al.[10] proposed the semantics aware malware detection algorithm that can detect variants of malware. The deficiency of malware detection by using pattern matching approach was overcome in this type of malware detection method.

Junfeng Wang et al.[11] proposed the mining format information technique of PE files to identify the malware. The in-depth analysis of static format information of PE files was performed.

I. Mohanty et al.[12] proposed the live forensic analysis approach to recover the digital evidences from the RAM of the victimized computer system. The tools used to acquire the memory dump is Nigilant 32 which is very expensive tool.

Y. Kim, S. Lee et al.[13] proposed live memory analysis technique to extract the registry entries associated with windows processes.

Different Approaches of Volatile Memory Analysis:

Volatile memory forensics have recently gained more focus as it can be granted as an effective resource to obtain more accurate evidences to find out the cyber criminals[12]. The digital evidences obtained from RAM analysis of victimized computer system can be obtained by mainly 2 approaches:

1. Live Response Approach
2. Memory Image Approach

Live Response Approach of RAM Analysis is the conventional way where the forensic investigator establishes a trusted shell in the victimized machine to load the trusted compiled libraries and software so as not to rely on completely to collect the digital evidences out of the system. The binaries of the attacker and the libraries used by forensic investigator both use the system call to contact the kernel[2]. The Live Response approach is not much reliable as there are few chances of the alteration of the memory artifacts due to loadable modules of the software installed on the victimized system for investigation. Also, the Live Response approach would not allow the investigator to repeat few procedures to acquire more accurate evidences. The Live Response Approach cannot perform the analysis of the hidden or terminated processes [2][12]. Memory Imaging Approach besides allows forensic investigator to acquire the RAM Image or dump using the Memory Imager forensic tool. The dump is then analyzed using memory forensic tools to find out the required memory artifacts to obtain the digital evidences. The advantage of Memory Imaging Approach is, it does not load additional modules on victimized system, it performs only a single action of capturing the Image of the system[2].The offline Memory Image Analysis approach is the repeatable process can be followed to obtain more accurate digital evidences as and when required additionally by the court.

Table 1 summarizes different approaches of memory analysis:

Title	Methodology Used	Scope of Work	Scope of Improvement
The Acquisition and Analysis of Random Access Memory,Timothy Vidas, 2007 Journal of Digital Forensic Practice(Taylor & Francis)	RAM Analysis using RAM Duplication Technique	To gather some relevant information most of the time the non-volatile storage media is required	Disk Forensics technque can be used to obtain the relevant information about the memory artifacts
Comparative Analysis of Volatile Memory Forensics,Amer Aljaedi et al. 2011, IEEE International Conference on Privacy,Security, Risk and Trust IEEE Conference on Social Computing,	Memory Image Analysis	Analysis of the processes and internet artifacts. Chances of being overwritten of the Terminated and cached processes	Memory imaging approach to analyze more memory artifacts like hidden processes, system log files, passwords, network logs etc. can be used.1
In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes, Robert J. et al.,2016 ,Journal of Forensic Sciences, In-Depth	RAM acquisition tools like Memory Reader & Belkasoft	Time consuming Command line approach of forensic investigation can affect the processing time of investigation	GUI based tools can be used to make the investigation process quicker to avoid more time consumption of command line tools
A study of Forensic & Analysis Tools,Sriram Raghavan et al., 2013 IEEE Sponsored by Louisville Chapter	Memory artifacts for digital evidence composition using FS metadata	Most of the memory forensic tools aquire FS metadata one at a time instead of grouping them for analysis	Grouping of relevant memory artifacts and identification of metadata based association can be achieved using FIA and FACE architecture
Forensic Tools For Investigating Cyber, 2016, Ala Berzinji, Asian Journal f Natural & Applied Sciences	Use of distinctive forensic tools like DumpIt, FTK	Lack in Cyber Forensic methodologies to find related memory artifacts	Digital evidence can be obtained using the data structure located in memory
Review of Live Forensic Analysis Techniques, 2015 Shuaibur Rahman et al., International Journal of Hybrid Information Technology	Live Response forensic analysis method	Chances of losing the important digital evidences in case of corruption of the victimised system	Memory Imging approach can be used to achieve the repeatable investigation process to get the relevant digital evidences
Design and Implementation of a Live-analysis Digital Forensic System	Live-analysis method	Shut down or unavoidable reboot may result into unacceptable restoring of the current state of the system	Dead analysis approach or memory imaging approach can be prefered for investigation.

Table 1:Different approaches of memory analysis

The open source memory forensic tools for Memory Imaging and Memory dump analysis often use the commands to obtain the desired memory artifacts. Most of the time to remember the long sequences of commands may result into the time-consuming task of getting the things to be done within stipulated time period. The most powerful memory analysis tool is Volatility, which prefers the command line approach (CLI) for its use.

In this paper the CLI approach of the memory analysis is completely replaced by the GUI Framework that offers much more flexibility to forensic investigator to obtain the result on a single click event getting the results quickly as compared to command line approach to save time to get the evidence.

Table 2 represents the comparison of few Forensics Tools:

Tools	GUI Support	Digital Artifacts Analysis				Operating System Support	Open Source
		File system examination	Memory dump examination	Logs examination	Packet capture examination		
Encase	Yes	√	√	X	X	Windows	X
FTK	Yes	√	√	X	X	Windows	X
Sleuthkit	No	√	X	X	X	Windows/ Linux	√
PyFlag	Yes	√	√	√	√	Linux	√
Volatility	No	X	√	X	X	Windows/ Linux	√
Autopsy	Yes	√	√	√	X	Windows/ Linux	√
OSForensics	Yes	√	√	√	X	Windows/ Linux	√
CAINE	Yes	√	√	√	X	Windows	X

Table 2: Comparison of few forensics tools

In the recent era digital resources like computer systems, mobiles, tabs etc. are more prone to be attacked or compromised by the different types of viruses, worms and Trojans. Digital forensics is very useful to identify such offensive attacks by providing various techniques to determine the origin of incidents like cybercrime. Different techniques of detecting the malwares were proposed to find out these malwares from the computer system. As the malwares got entry into the system they become active to infect the number of processes as well as other memory artifacts. The malware detection approaches involves two basic methodologies:

1. Static malware detection
2. Dynamic malware detection

Basic static analysis examines malware without viewing the actual code or instructions. The static analysis method can provide the information about malware like file name, MD5 check sums or hashes, file type, file size and recognition by anti-virus detection tools.

Basic dynamic analysis actually runs malware to observe its behavior, understand its functionality and identify technical in- dicators which can be used in detection signatures. The dynamic analysis of malwares can provide the information about malware like file path locations, registry keys, and additional files on the system or network.

Table 3 summarizes the different malware detection techniques used by some authors:

Title	Methodology Used	Scope of Work	Scope of Improvement
Automated Behavioral Analysis of Malware 2017 The article is accepted and published by United States Government [17].	Malware analysis using Cuckoo sandbox	Malware Analysis were carried out using Cuckoo Sandbox to identify the behavior and propogation of the malware.	The more accurate behavior of the malware can be analysed using automatic pattern generation.
A statistical model for undecidable viral detection,2007, Eric Filiol et al., Springer-Verlag France[18].	Statistical Approach of malware detection	The approach was used for automatic signature generation by analyzing exectuble file's code.	The approach was not suitable for large malware famiy with statistical analysis.
A Malware Detection Scheme Based on Mining Format Information, 2014,Jinrong Bai et al., Scientific World Journal[19].	Mining format information of Portable Executable (PE files) is used.	Some features from format information of PE files are used.	Mining format information of only PE files were used. Static approach of malware analysis leads to restriction on analysing the highly accurate detection of malware families.
Optimised Malware Detection in Digital Forensics,2014,Saeed Almarri et al.,International Journal of Network Security & Its Applications (IJNSA)[20].	Static and Dynamic analysis methodlogies of malware detection were carried out using Forensic Tools like Sleuth Kit and Autopsy.	Static Analysis for classifying the file format, analyzing strings were performed. Dynamic analysis to investigate registries, running processes and running services were done to detect malwares.	More open source tools with the behavioral pattern and signature scanning methods can be used to detect more advanced malwares.

Table 3: Different malware detection techniques

Digital forensics investigation is a process of incident response to assess and present the digital evidence which must be admis- sible in court [6].

The Following step may involve following steps are involved in a forensic investigation:

1. Data acquisition from volatile memory is performed either by using Live Response approach or memory imaging approach.

2. It is to be taken care of about the original artifacts from volatile memory not to be got tampered with as it may cause negative impact on the investigation process.

3. Hashing is performed after acquisition step to check the integrity of the original evidences.

4. The original evidences is stored in a secured location preferably that would not be easily accessible.

5. The image of volatile memory is created sometimes in memory imaging approach of memory analysis to search and recover the deleted data.

6. The strong forensic report is prepared that describes the forensic method, tools used and the root cause of crime in an authentic manner in the court of law.

III. METHODOLOGY

A. System Architecture

The system analyzes the malicious processes from a memory dump, using the GUI based forensic toolkit developed in this project. This toolkit includes the memory image analyzer like Volatility Framework and YARA signature scanner tool. The Volatility Framework is totally open source tool , implemented in Python under the GNU General Public License (GPL v2). It is used for the extraction of digital artifacts from volatile memory (RAM) samples. These frameworks provide a complete command line interface to an investigator. The command line oriented tool provides a wide range of functionality to extract certain artifacts from a RAM samples like event logs, files, information of loaded DLL's, open network connections, open registry handles etc. The target of this project is to provide an extension to Volatility Framework i.e. a GUI based approach to analyze the memory dump and extract the malicious processes.

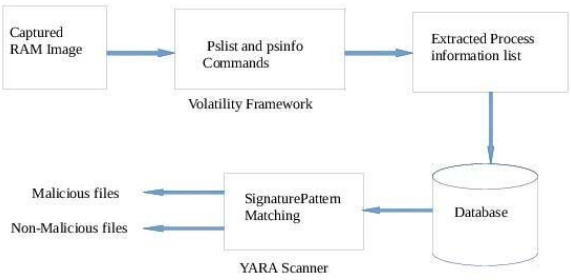

Fig. 1System Architecture

B. Work Flow of the System

1) Phase-I Volatile Memory(RAM) Image Acquisition: Volatile memory image of a compromised or victimized computer system can be acquired using a forensic tool like DumpIt, LiME. Volatile memory artifacts from this image will be analyzed for identification of malicious processes.

2) Phase-II RAM Image Analysis: In a memory imaging analysis process the volatile data like system logs, network logs, registry files, running processes of the system are analyzed using the Volatility forensic tool. The tool runs the plugin like psinfo and pslist to identify the process information details and list of the processes respectively from the memory image.

3) Phase-III Storing the process information into the database: The analysis of RAM image provides the process information details; these details will be stored into the database for its later use in identifying the malicious processes using a Scanner tool like YARA Scanner.

4) Phase-IV Pattern matching process:

Information of processes and files from memory image will be provided to the YARA Scanner tool, which works on pattern matching rule. User defined rules of YARA Scanner will be written to compare the signature of a file. To identify the malicious processes, YARA Scanner works upon pattern matching of file signature. The user defined rule of YARA Scanner file will contain the specific signature pattern which will be compared with the signature of the files extracted from the memory image. If the signature mismatches or viewed to be tampered then the corresponding file will be categorized as a malicious file.

5) Phase-V Report Generation: User defined rules of the YARA Scanner tool will process the files extracted from RAM Image and it will return the malicious and genuine processes to the user. The report of malicious processes will be generated for further malware analysis.

The paper proposes a method for detecting and extracting the malicious processes from RAM Image, the rule-based approach of pattern matching is used. The open source YARA Scanner allows to write the rules based upon the signature pattern of the files. The rule-based approach is the dynamic analysis method of malware detection where the rule file of the YARA Scanner is matched against with the files from the RAM Image during the analysis procedure.Yara is a tool that helps us to identify and classify malware software samples by the use of rules. It is an open source tool that can work on multiple platforms and can be used from both command line interface(CLI) or using a Python script. In this project the YARA scanner is integrated in a GUI framework that provides flexible use of this tool without much overhead of remembering commands to execute the operation.

Syntax of YARA rules
rule rule_ name
{
strings:
$test string1= “Testing”
$test string2= {E1 D2 C3 B4} Conditions:
$test string1 or $test string2
}

Strings: This section contains the strings/pattern/signature that we need to match against a file. It can be Hexadecimal string and may contain wild card combinations along with it or text string in the form of ASCII text that can be matched up with condition set.

Conditions: Conditions sets evaluate Boolean expressions.

C. Algorithm

Input: Directory { Extracted files1,files2,.....file n } Output: Evidence Report Malicious files
Define: String pattern = $String in YARA file File Signature Header= HDString
Step1: Set the string match pattern in YARA file. Step2: Compare the $String with HDString Step3: if
$String is equal to HDString then Matching found; classify the file as malicious file
else
File is non-malicious
Step4: Repeat the procedure for complete directory input

D: Mathematical Model

Input : { P1, P2, P3 }
Functions: {f1, f2, f3 }
Output: {Malicious and Non-malicious Processes list} where P1, P2 and P3 are processes
Process: P1 (RAM Image creation)
{
Input: Capturing Running processes from volatile memory
f1: Processing with Image Analyzer
Output: RAM Image
}
Process: P2 (List of extracted processes)
{
Input: RAM Image
f2: Extraction of processes from memory dump to database Output: Process list with information
}
Process: P3 (Generation of evidence report)
{
Input: Extracted Process list from memory dump f3: Pattern matching from database
Output: list of malicious and non-malicious processes
}

E. Event Diagram
State/Event diagram:
Processes object={P1,P2,P3 }
Events={E1,E2}
Causes of events={f1,f2,f3}
Here the processes P1, P2 and P3 will be the

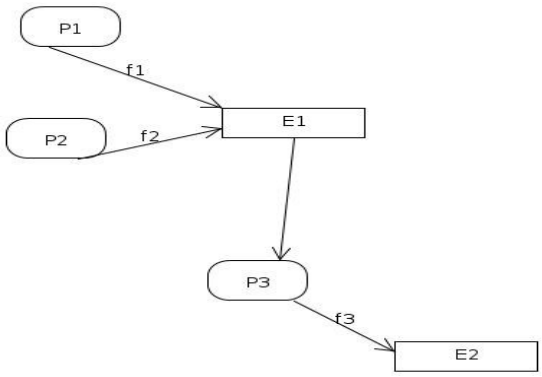

Fig. 2Event Diagram

IV. EXPERIMENTAL SET UP AND RESULT

The memory dumps of the malware affected victimized com- puter systems are collected to detect and extract the malicious processes. Most of the time the vital memory artifacts are identified as an entry point by the malware. In this experiment the sequences of phases are executed as explained in section III. In this experiment signature based identification of the malware is carried out using YARA Signature Scanner. The YARA Scanner uses the data set in the form of the file Strings that is written with a particular rule. Here the Strings of Ransomware and Stuxnet malwares are used to write the YARA rule files which are compared with the processes from RAM Images of the victimized or malware affected computer systems. The input data set, experiment procedure and the result are mentioned here.

Table no.5 shows the Experiment procedure.

The Experiment Procedure:

Data Collection and Procedure	1.Create the RAM Image of the victimised computer system. 2. Obtain the profile of the Operating System of victimised computer system 3. Show all the processes from the RAM image 4. Enlist the details of the every process to find the details of the processes 5.Collect the strings of malware samples of Stuxnet and Ransomeware. 6.Process the strings through HxD editor to analyze the suspecious strings. 7. Write the YARA rule using the strings of the malware files.
Scanning Process and Detection	1. Store all the RAM Processes into the database and scan it with YARA Scanner. 2. Compare all the processes from RAM against the YARA rule files.
Analysis	If the signature of the processes mateches with signature based YARA rule file, the process is identified as malicious process. Thus the malicious processes can be extracted.

Table 5:Experiment Procedure

Table no.6 describes the input data sets, memory artifacts and the extracted malicious processes

The Experiment Environment:

Host Operating System	RAM Dump Size Used	Operating System Profile detected	Malware	Associated Ransomeware SHA256	Extracted Malicious Process
Ubuntu-14.04.1-kernel-3.16.0-30-generic	536.9 MB	Windows OS XP2x86	Wannacry Ransomeware	59a3230782c6d74bcb8ff8bd4101db211f0f9ace82aa2af054915e4133b21cb2	WannaDecrypter.dmp Pid 1940
Ubuntu-14.04.1-kernel-3.16.0-30-generic	538.8MB	Windows OS XP3x86	StuxNet	5a8bd32d2a6414448da461f6c67197671c3b2e7e2b20e9ce32d4d4c966b4411b	1.lsass.exe Pid 680 2. lsass.exe Pid 868 3. lsass.exe Pid 1928

Table 6:Experimental Setup and Result

The sources of Malware sample used in this experiment are mentioned here.
https://tuts4you.com/e107 plugins/download/download.php? action=list&id=89
https://cyberarms.wordpress.com/2011/11/10/ memory- forensics-analying-a-stuxnet-memory-dump-and-you-can-too/
https://www.hybrid-analysis.com/sample/

The entry points and the affected DLL's are notified for collecting the digital evidence that can be further analyzed to find out the root cause of the cybercrime. Such kind of digital evidences play a vital role to prove the cybercrime in a court of law. YARA Rule for detecting the malware affected processes are written and the memory process scan is performed. The GUI based frame wok helps to get the result on the click event which can time saving for forensic investigator not to depend upon the long sequence of commands to remember. Few Screen shots from creation of the RAM Image till the extraction of the malicious processes using the GUI based Memory Forensics Toolkit are mentioned here.

1. Selecting the RAM Image of the victimized computer system. Forensic Investigator can select and upload the RAM Image that is already created using DumpIt Memory Image Creator tool.

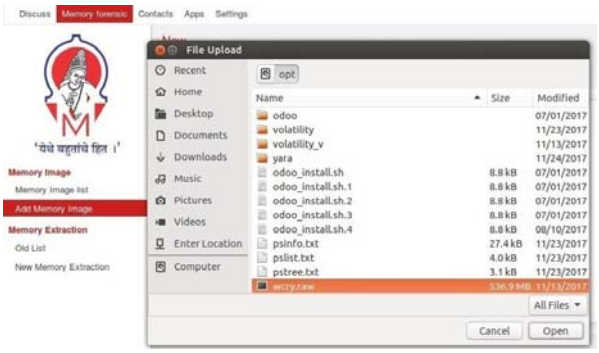

Fig. 3 Select the RAM Image to analyze

2. To extract all the processes from RAM into a database on which the YARA scanner will run.

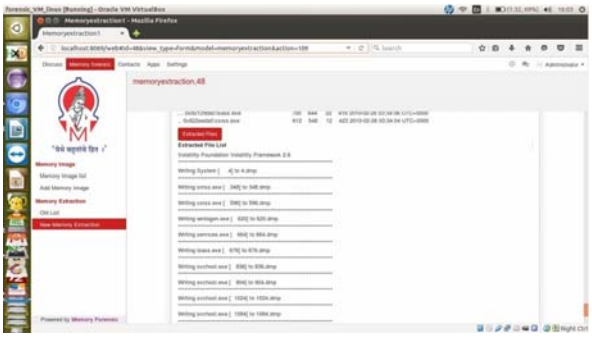

Fig. 4 Processes dumped into the database

3. To extract the malicious processes from the victimized computer system.

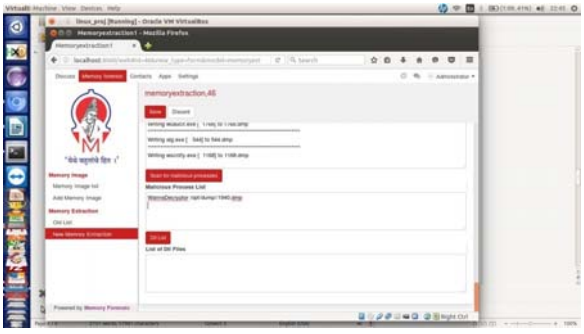

Fig. 5 Processes dumped into the database

V.CONCLUSION AND FUTURE WORK

In this work, different approaches of memory analysis and malware detection are reviewed and the most trustful approach to collect volatile memory artifacts that is Memory Imaging approach is preferred. Furthermore, due to increase in the cyber crimes an efficient approach of investigation must be followed in order to obtain the evidences as early as possible. To extract the malicious processes from RAM dump Signature based and String pattern matching rule-based procedure of the YARA scanner is used. Instead of following the command line method of volatility memory forensic tool to analyze the processes, GUI based automated forensics toolkit is used for the RAM analysis which can save the time of investigation. The proposed integrated tool provides rich GUI for memory analysis, scanning and extracting the malicious processes from RAM Image. In future the extracted processes can be sent for further investigation of malware using malware forensics to find out the root cause of the malware attack into the victimized computer system.

REFERENCES

[1] Timothy Vidas, 2007 Journal of Digital Forensic Prac- tice(Taylor Francis) The Acquisition and Analysis of Random Access Memory.

[2] Amer Aljaedi, Dale Lindskog, Pavol Zavarsky,Ron Ruhl, Fares Almari, 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE Conference on Social Com- puting, Comparative Analysis of Volatile Memory Forensics.

[3] Robert J. McDown, Cihan Varol, Leonardo Carvajal and Lei Chen,2016 Journal of Forensic Sciences, In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes.

[4] Sriram Raghavan, S V Raghavan 2013 IEEE Sponsored by Louisville Chapter, A study of Forensic Analysis Tools.

[5] Ala Berzinji, Asian Journal f Natural Applied Sciences, Sept.2016 Forensic Tools For Investigating Cyber Crimes.

[6] Ezer Osei Yeboah-Boateng, Elvis Akwa-Bonsu 2016 Journal of Cyber Security, Digital Forensic Investigation: Issues of In-tangibility, Complications and Inconsistencies in Cyber-Crimes.

[7] Elick Chan, Winston Wan, Amey Chaugule, Roy Campbell 2016 Publication on ResearchGate, A Framework for Volatile Memory Forensics.

[8] Arpit Patel, Nilay Mistry, 2013 International Journal for Scientific Research Development, An Analyzing of different Techniques and Tools to Recover Data from Volatile Memory.

[9] Shuaibur Rahman, M.N.A. Khan, 2015 International Journal of Hybrid Information

Technology, Review of Live Forensic Analysis Techniques.

[10] Felex Madzikanda, Talent Musiiwa, Washington Mtembo, 2013 International Journal of Computer Science and Technology, Computer Forensic Considerations and Tool Selection Within an Organization.

[11] Aaron Walters, Nick L. Petroni 2007 White Paper at Komoku Inc., Volatools: Integrating Volatile Memory Forensics into digital Investigation Process.

[12] Abes Dabir, Abdel Rahman Abdou, Ashraf Matrawy, 2016 International Journal of Information and Computer Security, A Survey on Forensic Event Reconstruction System.

[13] I. Mohanty, and R. L. Velusamy,2012,International Journal of Security, Privacy and Trust Management, Information Re- trieval From Internet Applications For Digital Forensic.

[14] Y. Kim, S. Lee, and D. Hong,2008,ICST Proceedings of the 1st international conference on Forensic applications and techniques intelecommunications, Suspects' data hiding at remaining registry values of uninstalled programs.

[15] G. Palmer. A road map for digital forensic research. Technical report, Report from the Digital Forensic Research Workshop (DFRWS), November 2001.

[16] Sunghyuck Hong and Sungjin Lee,2015,Indian Journal of Science and Technology, New Malware Analysis Method on Digital Forensics.

[17] Qian Chen, Robert A. Bridges,2017,arXiv preprint arXiv:1709.08753v1, Automated Behavioral Analysis of Malware.

[18] Eric Filiol and S ébastien Josse,2007,Springer-Verlag France, A statistical model for undecidable viral detection.