RAM Forensics: The Analysis and Extraction of Malicious processes from memory Image using GUI based Memory Forensic Toolkit

Mr. Vivek Ravindra Sali
Dept. of Computer Engineering
Marathwada Mitra Mandal's
College of Engineering
Karvenagar, Pune
vivekravindrasali@gmail.com

Mrs. H.K.Khanuja
Dept. of Computer Engineering
Marathwada Mitra Mandal's
College of Engineering
Karvenagar, Pune
harmeetkaurkhanuja@mmcoe.edu.i
n

Abstract— In today's world the use of internet and information technology has grown up very rapidly. Due to increasing use of Internet the amount of cyber crimes have been increased. Hence it's become a very challenging task for the cyber crime investigator to not only finds out the root cause of the crime but also to prove it correctly in the court of law. Computer Forensics is the science of investigating the computer system to obtain the digital evidences to find out the root cause of cyber crimes. 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 as 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.

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, cyber crimes have been increased. Cyber crime is any illegal activity which involves a computer system or its related systems or their applications. Today solving any cyber crime 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, cryptographickeys, process information and other vital data related to number of processes running in a ystem[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 cyber crime[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 make 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 from the processes of memory image dump, 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. It uses the efficient pattern-matching rule. YARA supports the use of three different types of strings for pattern-matching:

(a) Hexadecimal Strings

978-1-5386-5257-2/18/$31.00 c 2018 IEEE

(b) Text Strings based on ASCII text
(c) Regular Expressions

In this paper the out of above mentioned few tools, DumpIt, Volatility and YARA Scanner tool are used to perform an analysis of the RAM Image to retrieve the relevant memory artifacts like processes. The User can write set of rules for YARA Signature Scanner to find the malicious processes. The rule includes text strings, Hexadecimal Strings and regular expressions which contains file signature pattern of ".exe" file of the malware.

II. Review of literarure

Timothy Vidas [1] discussed about the benefits and drawbacks of traditional incidence response methods.

Methodology Used: RAM analysis using RAM duplication technique.

Scope of Work: RAM Duplication technique 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

Scope of Improvement: Disk Forensics technique can be used to obtain the relevant information about the memory

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.

Methodology Used: Memory Image Analysis.

Scope of Work: Analysis of the processes and internet artifacts. There might be chances of being overwritten of the Terminated and cached processes.

Scope of Improvement: In memory imaging analysis process the vital evidences like cached processes, some Internet artifacts can be extracted directly from the memory dump. Also more memory artifacts like hidden processes, system log files, passwords, network logs etc. can be analyzed from memory image.

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, were compared in the study.

Methodology Used: RAM acquisition tools like Memory Reader Belkasoft are used.

Scope of Work: The Command line approach of forensic investigation can provide information about the parameters like total execution time, platform limitations, reporting capabilities, shared and proprietary DLLs, modified registry keys and invoked files through the analysis.

Scope of Improvement: The command line tools use may affect on increase in time required for investigation process. The GUI based tools can be used to make the investigation process quicker to avoid more time consumption in remembering the need of complex sequences of commands.

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.

Methodology Used: Memory artifacts for digital evidence composition using FS meta data.

Scope of Work: The study highlighted the importance of meta data and its use across the heterogeneous sources of digital evidences. Most of the memory forensic tools acquire FS metadata one at a time instead of grouping them for analysis.

Scope of Improvement: Grouping of relevant memory artifacts and identification of meta data based association can be achieved using FIA and FACE architecture.

R. Raines et al.[5] 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.

Methodology Used: Obtaining the file Strings of PE files using HexDump tool.

Scope of Work: Pattern recognition techniques can play a substantial role in malware detection especially in cyber situation awareness and assurance. The MaTR system uses a straightforward process for detecting malware using only a program's high-level structural data.

Scope of Improvement: The hybrid solution using MaTR approach and other static heuristic approaches like KM retest and commercial antivirus product can provide the 100% detection of unknown malware samples.

A] 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 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. 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 offline to obtain the digital evidences.

Digital forensics is very useful to identify such offensive attacks by providing various techniques to determine the origin of incidents like cyber crime. 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 indicators which can be used in detection signatures. The dynamic analysis of malwares can provide the information about malware like file path locations, registry keys, additional files located.

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. This framework provides 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.

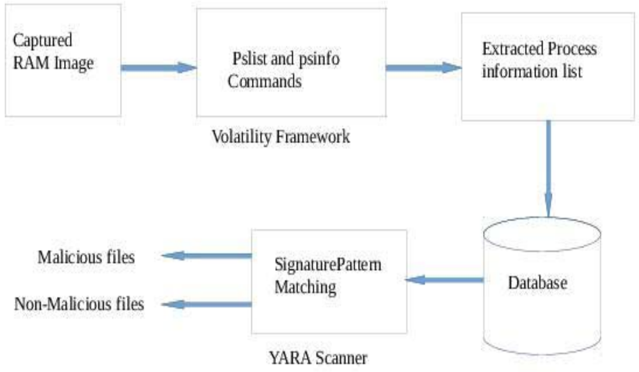


Fig. 1 System Architecture

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 etc.
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.
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.
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.

Syntax of YARA rule:

```
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: 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

Processes Objects= {P1, P2, P3}

Events= {E1, E2}

Causes of events= {f1, f2, f3}

Here the processes P1, P2 and P3 will be the processes acts as objects which cause an event. Process P1 and P2 cause an event E1 by using function f1 and f2 respectively. This event E1 changes the state of process P2 to process P3 which in turn cause a new event E3 to be occurred. This event determines the malicious process out of the genuine processes.

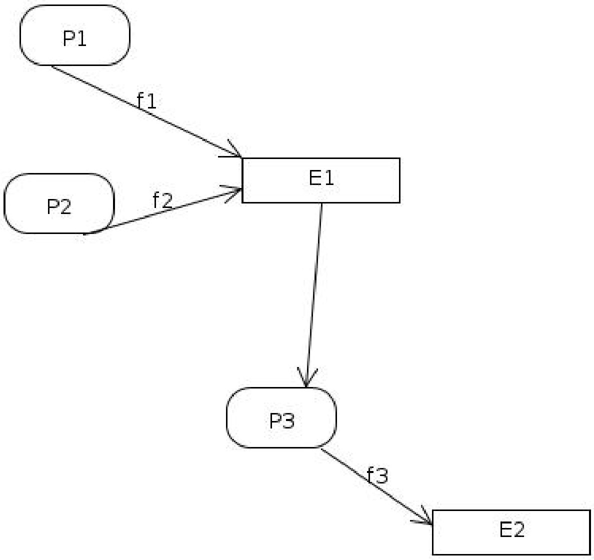


Fig. 2 Event Diagram

IV. EXPERIMENTAL SET UP AND RESULT

The memory dumps of the malware affected victimized computer systems are collected to detect and extract the malicious processes. 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 computer system. After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

Experiment Procedure

Data Collection And Procedure	1.Create RAM Image of victimized computer System. 2.Obtain Profile of OS 3.Display Detail Information of all Processes from RAM Image. 4.Collect the File Strings & File Signature of Ramsomware & Stuxnet malware 5. Write the YARA rule-set.
Scanning Process And Malicious process Detection	1.Strore all the dump files (processes from RAM Image) into Local Storage device and Database. 2.Compare file strings & file signature of dump Files with the YARA rule set defined.
Analysis	If the File Strings and File Signature mentioned into the YARA rule set matches with file strings & file Signature of the any of the dump files. The respective file in-turn the process is classified as malicious process.

Table 5: Experiment Procedure

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

Experiment Environment

Host OS	**RAM Image Size**	**OS profile Detected**	**Malware Samples**	**Extracted Malicious Processes**
Ubuntu 14.041-Kernel-3.16.0-30-generic	536.9MB	Windows OS XP2x86	Wannacry Ransomware	WannaDecrypter.dmp Pid 1940
Ubuntu 14.041-Kernel-3.16.0-30-generic	538.8MB	Windows OS XP3x86	Stuxnet	1.lsass.exe Pid 680 2.lsass.exe 868

Table 6: Experimental Setup and Result

V. EXPERIMENT PROCEDURE

1) Registration Authentication Process:

The registration and authentication process is carried out by the forensic investigator which is mandatory to avoid the mis-use of the tool. On successful authentication the forensic investigator gets the privileges to use the functionalities of the tool.

2) RAM Acquisition Process:

In this experiment procedure the Memory Imaging approach of volatile memory forensic investigation is used. The RAM Images of both guest VM's are captured for analysis.

3) Determine OS Profile Information:

The profile information of the operating system were determined. The Profile Information determines the type of OS used which is necessary to obtain the important memory artifacts from the memory.

4) RAM Image Analysis Process:

The processes from the RAM Image of the malware affected or victimized VM were analyzed to get the detail information about each process like process name, process ID, path of the process, parent-child relationship between processes etc. The path and name of the uploaded RAM Images were stored to the database.

5) Dumping the processes from RAM Image:

The processes from the RA M image was extracted and dumped into the local storage and to the database for the future reference.

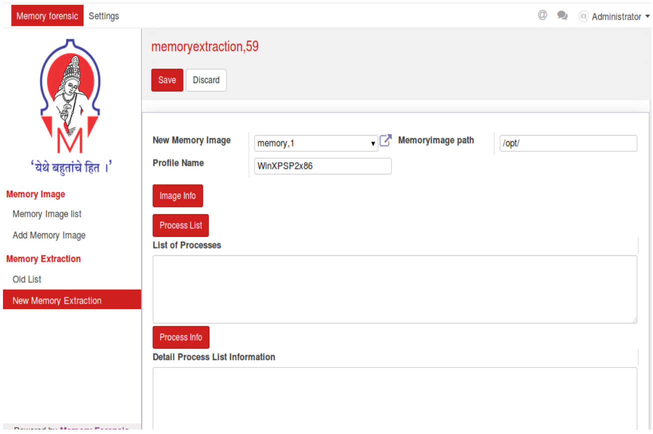
6) Extraction of the Malicious Processes:

The memory dump created was used to scan the dump files to obtain the malicious processes. The scanning was performed by user defined “YARA rule-file” containing the patterns of Signature and file Strings. The “YARA rule file” try to match the signature and file Strings pattern of each dump file using the rule defined in the “YARA-rule file”.

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 of the result are displayed here:

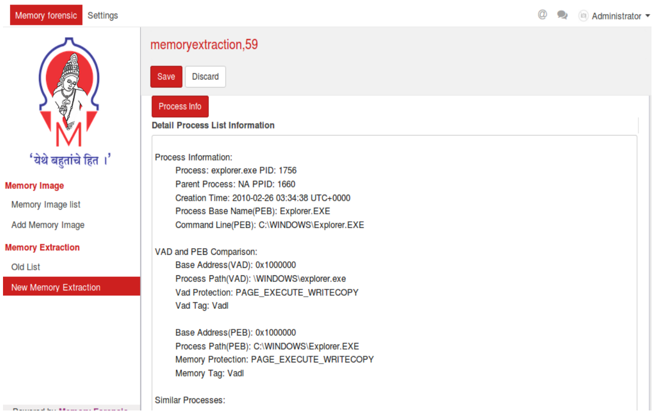
1. Determine the Operating System Profile for the analysis of volatile memory artifacts



New Memory Image: memory,1
MemoryImage path: /opt/
Profile Name: WinXPSP2x86

Fig. 3 Display Image Profile Information

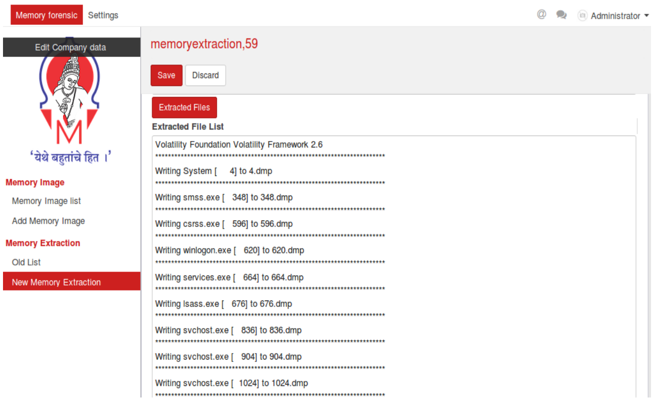
2. Obtaining the Detail information of the processes for the analysis



```
Process Information:
     Process: explorer.exe PID: 1756
     Parent Process: NA PPID: 1660
     Creation Time: 2010-02-26 03:34:38 UTC+0000
     Process Base Name(PEB): Explorer.EXE
     Command Line(PEB): C:\WINDOWS\Explorer.EXE

VAD and PEB Comparison:
     Base Address(VAD): 0x1000000
     Process Path(VAD): \WINDOWS\explorer.exe
     Vad Protection: PAGE_EXECUTE_WRITECOPY
     Vad Tag: Vadl

     Base Address(PEB): 0x1000000
     Process Path(PEB): C:\WINDOWS\Explorer.EXE
     Memory Protection: PAGE_EXECUTE_WRITECOPY
     Memory Tag: Vadl

Similar Processes:
```

Fig. 4 Display the details of the processes

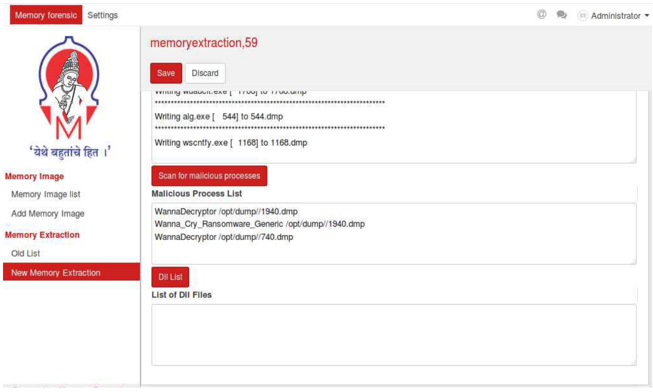
3. Creating the Dump files of the processes from RAM Dump storing them on a local storage as well as into Database



```
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing System [     4] to 4.dmp
************************************************************************
Writing smss.exe [   348] to 348.dmp
************************************************************************
Writing csrss.exe [   596] to 596.dmp
************************************************************************
Writing winlogon.exe [   620] to 620.dmp
************************************************************************
Writing services.exe [   664] to 664.dmp
************************************************************************
Writing lsass.exe [   676] to 676.dmp
************************************************************************
Writing svchost.exe [   836] to 836.dmp
************************************************************************
Writing svchost.exe [   904] to 904.dmp
************************************************************************
Writing svchost.exe [  1024] to 1024.dmp
************************************************************************
```

Fig. 5 List of Dump files of the processes from RAM Dump

4. Scanning the dump files by the user defined YARA-rule to extract malicious processes.



```
************************************************************************
Writing alg.exe [   544] to 544.dmp
************************************************************************
Writing wscntfy.exe [  1168] to 1168.dmp
```

```
WannaDecryptor /opt/dump//1940.dmp
Wanna_Cry_Ransomware_Generic /opt/dump//1940.dmp
WannaDecryptor /opt/dump//740.dmp
```

Fig. 6 List of malicious processes

VI. 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 Practice (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 Computing, 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] R. Raines et al.,Wright-Patterson AFB, OH, USA,, Air Force Research Laboratory, Wright-Patterson AFB, OH, USA,Journal of Computer and Security,2011.

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

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

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

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

[10] Shuaibur Rahman , M.N.A. Khan , 2015 International Journal of Hybrid Information Technology, Review of Live Forensic Analysis Techniques.

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

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

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

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

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

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

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

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

[19] Eric Filiol and S˜Ac bastien Josse,2007,Springer-Verlag France,A statistical model for undecidable viral detection.

[20] Jinrong Bai,Junfeng Wang and Guozhong Zou,2014,The Scientific World Journal, A Malware Detection Scheme Based on Mining Format Information.

[21] SaeedAlmarri and Dr Paul Sant,2014,International Journal of Network Security Its Applications ,Optimized Malware Detection in Digital Forensics