Volatile Memory Acquisition and Extracting of Data Using Volatility Framework and Web GUI Application

N Sai Vaibhav, D Haritha

Abstract: ***Volatile memory plays a major role in live memory investigation, for the analysis of volatile memory, most of the investigators use Volatility Framework. In this paper, we are going to present how to extract the RAM memory from the suspected systems also preserving it using data acquisition tools and a Web GUI application using Volatility Framework.***

It also displays the extracted data as tables in the web page. It creates an easy approach for the investigators to do analysis by extracting the information from the volatile memory and also exporting that information as SQLite tables.

Index Terms**:** ***Digital Forensics; Volatile memory; Non-Volatile; RAM Dump; Artifact; Acquisition***

I. INTRODUCTION

The investigation of volatile memory became more crucial than normal digital assets. The reason is that the RAM contains so many artifacts that tell about the running system. By extracting the RAM dump, it is possible to find more or less 70% of the information that relates to the purpose of investigation. Only by following the procedure to extract the RAM memory from the suspected system, it can be done.

This Dump contains lots of information like Running processes and services, System information, Data about logged in users, Registry details, network connections, Running malicious codes.

Volatility framework is a widely used open source tool for the extraction of artifacts from the dump and also gives instant output. But what happens is it only works in CLI (Command Level Interface), that means for every artifact that we need to extract from, we have to give the command and then only it shows the data in the terminal itself. Most of the investigators get shorthanded with the disability of using complex commands in CLI. Therefore, the valuable tool became unused by investigators and one more problem is a correlation of extracted data and saving it.

This paper presents a Web Graphical User Interface (GUI) and extension for the volatility framework. Which can overcome the problems mentioned above and make the process of investigation easier. GUI can also use to correlate the output from the dump and creates a format to save the date.

This paper is enclosed with the following topics, what is Digital Forensics, steps to follow in the process of investigation, the difference between volatile and non-volatile

memory, memory dump acquisition, working with GUI.

II. DIGITAL FORENSICS

Digital forensics is a part of normal crime forensics where it is useful is whenever the system or any digital assets is a part of a crime. Doing an investigation on digital devices like computers, mobiles, digital gadgets like smartwatches, iPads, cameras, etc.

Digital forensics has also divided into sub-branches based on the type of digital assets like Mobile Forensics, Computer Forensics, Malware Forensics, Cloud Forensics, Network Forensics, Memory forensics, etc., all these are part of Forensics investigation.

The main motive of digital forensics is the extraction of data that is stored in digital format and making it understandable and protecting the data from tampering and storing the data for investigation.

III. STEPS TO FOLLOW IN DIGITAL FORENSICS

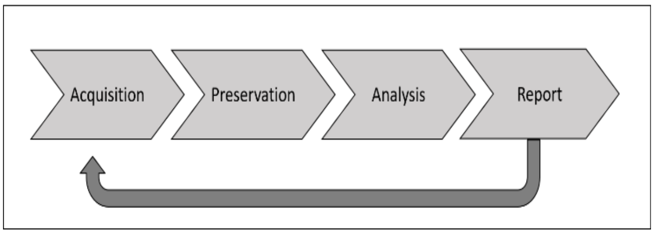


Fig 1: Digital Forensics Process

Fig:1 shows the process of digital forensics. The first step is Data Acquisition. In this step, we need to collect the potential data from assets by cloning or imaging techniques. The digital devices that are considered as evidence are hard disks, mobile devices, memory cards, etc., from all these devices we need to extract.

Note: Basically, there are two types of mirroring the data, Cloning, and Imaging. Cloning means creating the exact copy of the disk which can be used instantly without any conversions required. This type of copying is done mostly with the secondary storage devices like hard disks pen drives etc.,

Revised Manuscript Received on May 10, 2019.

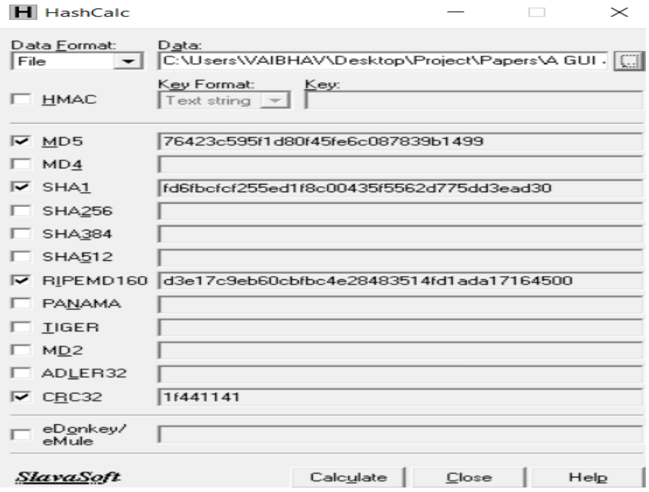
N Sai Vaibhav, M Tech Student**,** Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

Dr D Haritha, Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

The imaging means, creating an image file which we can't use instantly because the file is in encrypted form, so we must process it first and then we can see the file in it.

In the next step, the collected data need to be saved and protect from altering or tampering. It is accomplished by calculating the hash value of the evidence at the time of collection.

Hashing algorithm plays a very important role to ensure evidence integrity. Since most digital forensic tools either uses MD5 and SHA hashing algorithm. There is a tool called HashCalc make this work for us to calculate the hash values of any file.



HashCalc

Data Format: File

Data: C:\Users\VAIBHAV\Desktop\Project\Papers\A GUI .

□ HMAC

Key Format: Text string

Key:

☑ MD5 76423c595f1d80f45fe6c087839b1499

□ MD4

☑ SHA1 fd6fbcfcf255ed1f8c00435f5562d775dd3ead30

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160 d3e17c9eb60cbfbc4e28483514fd1ada17164500

□ PANAMA

□ TIGER

□ MD2

□ ADLER32

☑ CRC32 1f441141

□ eDonkey/eMule

Fig 2: Hash Calculator

The third step is analysis. In this step the data is examined, what file and folders are present and registry values, events, etc.,

In the last step, generating the report about what found in the assets with the process and include the extracted information details. The report format is based on the requirement.

IV. VOLATILE MEMORY AND NON-VOLATILE MEMORY

Volatile memory is a type of memory where the entire data vanishes as soon as the power is OFF. This type of memory is also called temporary memory. The real time example of Volatile memory is RAM (Random Access Memory).

Non-Volatile Memory is a type of memory that stores data permanently, the data is not lost even the power is turn OFF. Non-volatile memory is used for long time storage. The most common use of non-volatile storage is ROM or secondary storage like Hard disk, pen drive, memory cards, CD/DVD.

V. MEMORY FORENSICS

Memory Forensics also called live data forensics. It is defined as the process of analyzing volatile memory, The Live memory analysis includes investigation on advanced computer attack that managed to not to leave any traces on the system.

VI. MEMORY DUMP ACQUISITION

RAM memory acquisition is a very crucial part of Digital forensics. The investigator should rush to the system and start taking the dump before the system shutdown and use acquisition tools. There are so many open source RAM acquisition tools that helps to extract the RAM memory.

The most using tool for extraction is FTK Imager. It is an open source and also trusted tool for RAM dump extraction and also many forensics works like cloning and imaging the hard disk. Using FTK Imager investigator can able to create local and remote system images.

By using the FTK imager tool it creates a .mem file which is more size than the actual RAM of the system. Assume that the system ram is 2gb then the dump will be 2.5gb to 3gb and if RAM is 4gb then the dump may be 5gb to 6gb.

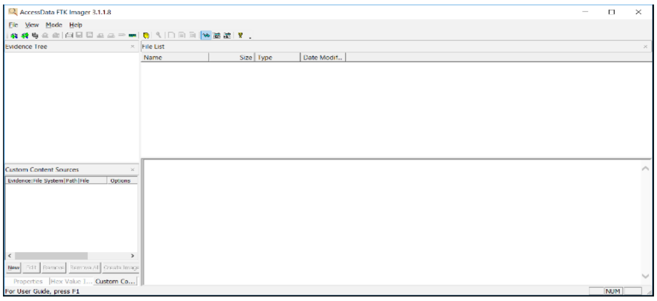


Fig 3: FTK Imager

FTK image can able to extract RAM from any version of windows operating system. It doesn't work for Linux or MAC.

For Linux system memory extraction there is another tool called LiME (Linux memory extractor) which is an open source tool.

VII. VOLATILITY FRAMEWORK

Volatility is an open source memory forensics tool kit, it is developed in python. It can perform analysis on RAM dump from 32bit/64bit systems. It supports analysis for Windows, Linux and also for MAC, Android. It is capable of performing monitoring running processes by using data found in the RAM. It can also do process listing, ports, network connections, etc., from the dump. This framework provides better efficiency of forensics research.

VIII. KEY FEATURES OF VOLATILITY FRAMEWORK

1) It can perform Analysis of 32bit/64bit systems.
2) It can run on window, Linux, MAC platforms that support Python
3) It supports memory formats like
4) Raw linear sample (dd)
5) Hibernation file
6) LiME format (when the dump is taken from Linux system)

7) Virtualbox Core Dumps, HPAK Format (FastDump), etc.,
8) It also supports Linux memory dump in raw or LiME formats.

IX. WORKFLOW

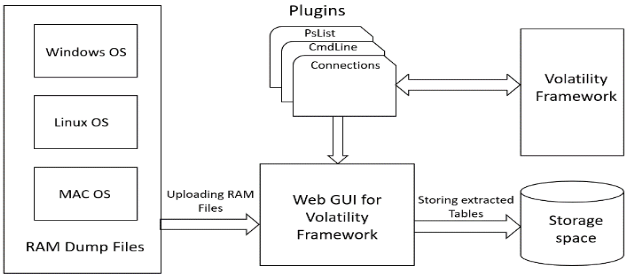


Fig 4: Work Flowchart of GUI

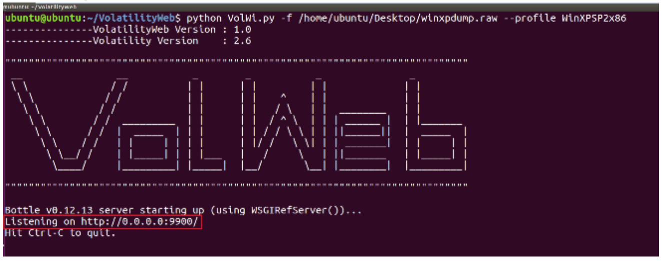
The workflow structure makes easy to understand the extended GUI for volatility framework. From Windows or Linux or MAC operating systems, we extract the RAM dump files with respective tools and uploading those files to GUI. The Volatility Framework contains different types of plugins each one has its unique purpose. Now the plugins are accessing using python script and display on the Web page based on the OS type.

Web GUI has a home page with a list of plugins along with a button to click. Then the plugin in runs in the backend and display its result on the page itself in a tabular format, also export the table to an SQLite database.

X. WEB GRAPHICAL USER INTERFACE FOR VOLATILITY FRAMEWORK

A. Installation Procedure:

This tool can be used in any python supported operating system with preinstalled volatility framework. It is a portable tool and needs only one command to execute and start working with.



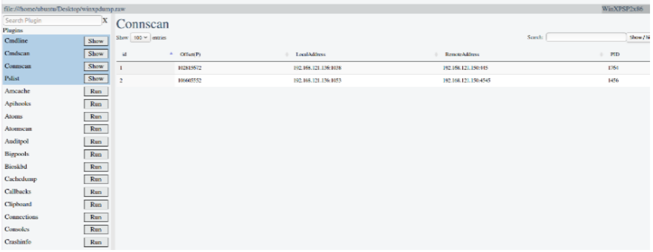
```
ubuntu@ubuntu:~/VolatilityWeb$ python VolWi.py -f /home/ubuntu/Desktop/winxpdump.raw --profile WinXPSP2x86
---------------VolatilityWeb Version : 1.0
---------------Volatility Version    : 2.6

Bottle v0.12.13 server starting up (using WSGIRefServer())...
Listening on http://0.0.0.0:9900/
Hit Ctrl-C to quit.
```

Fig 5: GUI Initiation

The given command executes the python script and hosts the web page locally, we can access it by using system IP address.

B. Working with GUI



file:///home/ubuntu/Desktop/winxpdump.raw WinXPSP2x86

Connscan

Show 100 entries Search:

id	Offset(P)	LocalAddress	RemoteAddress	PID
1	102815672	192.168.121.136:1038	192.158.121.150:445	1764
2	106605552	192.168.121.136:1053	192.168.121.150:4545	1456

Fig 6: GUI View

From the above Fig 6, the GUI contains fields, file path (where the RAM dump file is saved), type of system (the version of OS), list of plugins (only plugins compatible with the OS type) and output view.

XI. FUTURE SCOPE

Till this tool can use for Windows OS only, by adding additional profiles for Linux and MAC into the volatility framework it is possible to do analysis on Linux and MAC also.

XII. CONCLUSION

Using this process of extraction of data from RAM dump, the further analysis makes easy and performance of investigation gets faster. Also, for people with less knowledge in volatility can also use this process in their investigation.

REFERENCES

1. Periyadi1, Giva Andriana Mutiara1, Roni Wijaya1 (2017) “Digital Forensics Random Access Memory Using Live Technique Based on Network Attacked” ISBN: 978-1-5090-4911-0 (c) 2017 IEEE
2. Steffen Logen, Hans Höfken, Marko Schuba “Simplifying RAM Forensics A GUI and Extensions for the Volatility Framework”
3. Mary Geddes, Dr Pooneh Bagheri Zadeh “Forensic Analysis of Private Browsing”
4. K. Hausknecht, D. Foit, J. Burić; MIPRO (2015) “RAM data significance in Digital Forensics”
5. Matthew Simon Defence and Systems Institute (DASI) (2010) “Recovery of Skype Application Activity Data From Physical Memory”
6. Jaina J ER&DC Institute of Technology, (2015) “Extracting Network Connections from Windows 7 64-bit Physical Memory” ISBN: 978-1-4799-7849-6/15/$31. 00 ©2015 IEEE
7. Khaleque Md Aashiq Kamal, Mahmoud Alfadel and Munawara Saiyara Munia (2016) “Memory Forensics Tools: Comparing Processing Time and Left Artifacts on Volatile Memory” ISBN: 978-1-5090-5769-6/16/$31.00 ©2016 IEEE
8. Charl Meyers, Adeyemi R. Ikuesan, Hein S. Venter (2017) “Automated RAM analysis mechanism for Windows Operating System for Digital Investigation” ISBN: 978-1-5386-0725-1/17/$31.00 ©2017 IEEE
9. Ranul Thantilage, Neera Jeyamohan (2017) A Volatile Memory Analysis Tool for Retrieval of Social Media Evidence in Windows 10 OS based Workstations” 978-1-5386-2425-8/17/$31.00 ©2017 IEEE
10. Sunu Thomas, Sherly K.K, Dija S (2013) “Extraction of Memory Forensic artifacts from Windows 7 RAM Image” ISBN: 978-1-4673-5758-6/13/$31.00 © 2013 IEEE
11. Online “Volatlity Framework” github
12. Online “DATAINSIDER “What Are Memory Forensics? A Definition of Memory Forensics”
13. Online “Volatility Framework – Volatile memory extraction utility framework”
14. Online “Windows Memory Analysis with Volatility”
15. Online “LiME – Linux Memory Extractor” github
16. Online “SANS Digital Forensics and Incident Response Blog” SANS DFIR
17. Onine “Live Forensic Acquisition From Mac Computers”
18. Online “Volatility profiles for Linux and Mac OS X” github
19. Book “Practical Digital Forensics” by Richard Boddington

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*