Vol. 2 Issue I, January 2014
ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Volatile Memory Based Forensic Artifacts & Analysis

Rushita Dave[1] , Nilay R. Mistry[2], Dr. M. S. Dahiya[3]

Institute of Forensic Science

Gujarat Forensic Sciences University, Gandhinagar, Gujarat - India

Abstract: ***Today's technology grows its roots in positive and negatives both directions. Cyber criminals are always get one step ahead then the investigator. Digital forensics in the live environment is the biggest challenge. Aquistion of live artifacts on running system needs expertise to achieve expected results. One of the most important areas where every forensicator looks into is Memory, i.e. RAM - Random Access Memory. RAM is a volatile memory which flushes when system is shut down or restart. So before shutting down the system Memory dump should be taken. It is very important aspect for carving information resided into the volatile memory.[1] Here a role of a volatile memory analysis in digital forensics and the importance of the physical memory analysis is proposed. It is very useful in real time evidence acquisition analysis. Further we have introduced some of the tools and techniques used in acquisition and analysis of memory.***

Keywords— Memory Forensics; RAM Analysis; Artifacts; Live Forensics; Volatile memory artifacts

INTRODUCTION

Live memory acquisition and analysis does not have that much attention, which is given to other acquisition and analysis techniques in the area of digital forensics. Live Memory Analysis can be very much productive for analysis. Live Memory Analysis can give a large number of details. It requires a greater amount of care than the other methods of analysis. [2]

Live Memory Analysis plays an important role in the field of Digital Forensics. It can give the details about the running processes and applications in the system. Passwords can also be obtained using this analysis technique. The details, which are not stored on the hard drive of the system, can also be obtained with this technique. Live Memory Analysis can be very useful in Malware Analysis. Malware leaves some traces that can be analyze by live memory acquisition. [3]

MEMORY DUMP TOOLS FOR DIFFERENT OPRATING SYSTEM

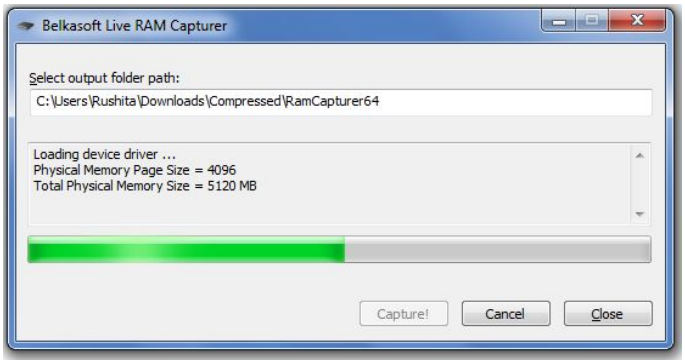
Here the list of memory aqusition tools for Windows/Linux/ Unix oprating system. That tools have capabilitites to fetch memory based potential evidences.[4] Random Access Memory fetching & dumping to specific directory process can be easy with the following tool.

WINDOWS BASED TOOLS

Belkasoft Live RAM Capturer

A free volatile memory forensic tool to dependably extract the entire content of the volatile memory of a computer. Memory dumps captured with this tool are generally analyzed using the tool of Belkasoft only named Live RAM Analysis in Belkasoft Evidence Center.

Vol. 2 Issue I, January 2014
ISSN: 2321-9653



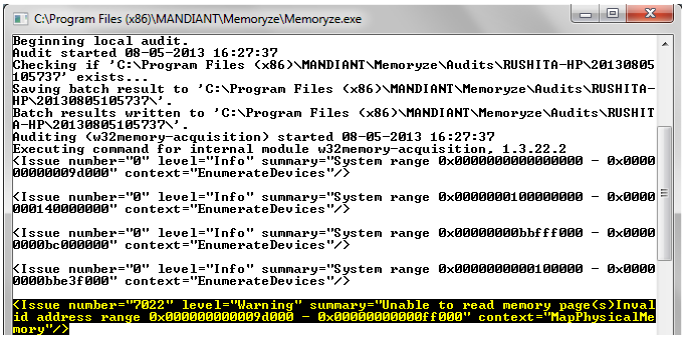
BELKSSOFT LIVE RAM CAPTURER

ManTech Memory DD

It acquires a forensic image of physical memory and stores it as a raw binary file. To check data integrity and help in the preservation of the evidence, the information captured by ManTech Memory DD is checked by the MD5. The binary file can be analyzed using outer tools to identify.

Mandiant Memoryze

Mandiant's Memoryze is free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis.



Belkssoft Live Ram Capturer

FTK Imager[11]

A tool that creates a forensic image of computer data without affecting original evidence and hashes for file integrity. FTK imager creates a bit-by-bit image, including unallocated space and slack space.

WinPmem

It is used for capturing raw memory images, Microsoft crashdump files for windbg and volatility. In this tool memory acquisition is done using MnMapIoSpace method.

Windows Memory Reader

It is a simple command-line utility to capture the contents of physical RAM. Results are stored in a Windows crash dump file or a raw binary file.

DumpIt

It is used to generate a physical memory dump of Windows machines. The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting.

Autopsy

It is open source digital investigation tool that run on Windows, Linux, OS X, and other Unix systems. It is used to analyze disk images and perform in-depth analysis of file systems.

LINUX BASED TOOLS

LiME

Linux Memory Extractor allows the acquisition of volatile memory from linux and linux based devices. LiME allows full memory captures from Android devices.

UNIX BASED TOOLS

Mac Memory Reader

It is a simple command-line utility to capture the contents of physical RAM, letting investigator to gather volatile state information. Results are stored in either a Mach-O binary file or a raw-format file

Mac Memory Dumper

Mandiant Mac Memory Dumper is a memory forensic program that allows the user to find incident responders in live memory. Mandiant Mac Memory Dumper can acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis.

Vol. 2 Issue I, January 2014
ISSN: 2321-9653

OSXPmem

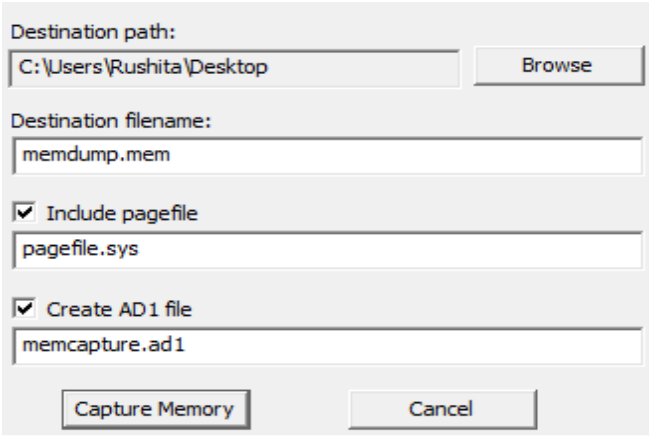
The OSX Memory Imager is an open source tool to acquire physical memory on an Intel based Mac. It consists of 2 components:

osxpmem - parses the accessible sections of physical memory and writes them to disk in a specific format.

pmem.kext - provides read only access to physical memory. After loading it into the kernel it gives a device file called /dev/pmem/ from which physical memory can be read.

CONCEPT OF MEMORY FETCHING & DUMPING FOR FORENSIC PURPOSE

While the discussion is going on the memory fetching some



concepts are required to be clear before starting the evidence analysis:

First: The memory dump must not be unintentionally altered by the investigator - for this issue dump memory with MD5 or SHA-1 hash for maintaining integrity of potential evidence.

Second: The stored memory dump is depends upon RAM Size and virtual paging. E.g. if RAM is 4 GB and by default virtual paging size is 2 GB then the 4 GB RAM dump is approx 6 GB. It includes virtual memory also while dump volatile memory.

ARTIFACTS IDENTIFIED FROM RAM ANALYSIS OF SYSTEM

Following artifacts can be fetch out from memory dump. [5]

Protected program details

Running processes and services

System information

Data about logged in users

Registry details

ARP cache and network connections

Fragments of conversation (chat), communication in social networks

Latest web browsing activities including private browsing detail,

Webmail system communication

Recently viewed multimedia

Running malicious codes

Passwords of the mail accounts

VOLATILE MEMORY CARVING & ARTIFACT ANALYSIS METHODOLOGY

Memory Capture

FTK Imager, a free tool is used to capture the RAM. The steps is performed as below,[9]

Go to “File” menu and select “Capture Memory

It will prompt a dialogue box where we have to choose destination path for the memory dump.[10]

We can also create pagefile.sys and AD1 file for analysis if needed.

Then select “Capture Memory”.

Memory capture GUI

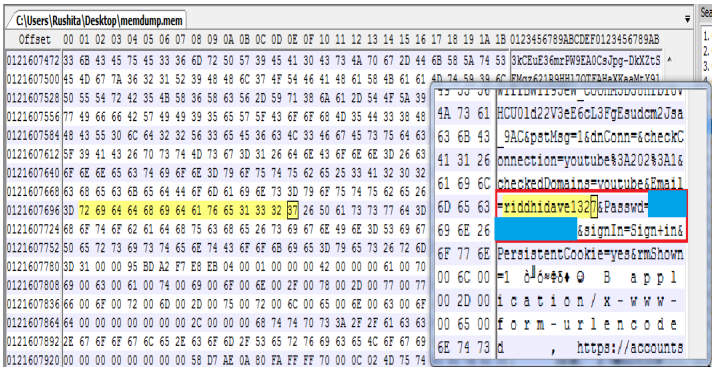
Memory Analysis

For analyzing the memory use any hex editor like WinHex or wxHexEditor. Autopsy forensic tool can be also used for the same. Here wxHexEditor is used for memory analysis.

Now open wxHexEditor and open the memory dump which you have taken form FTK Imager. It will show in 2 parts. On the right side we get the string values of information stored in

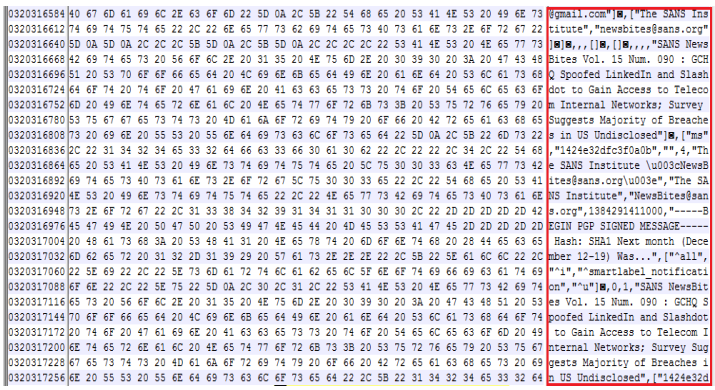
the memory and on the left side we will get the hex values for the strings to analyze the string values.

The search option is there for a particular query to find. So it will be easier for user to get the information quickly. Search can be done for the email accounts, services and processes running in the system, applications opened in the system. Here focus is on the most sensitive information and that is the credentials of email accounts and other social networking accounts.



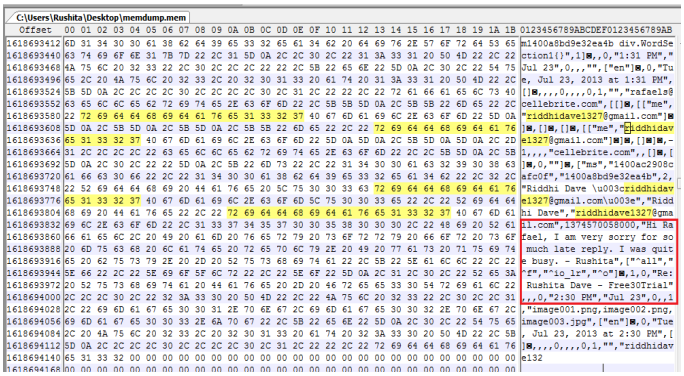
Gmail Username and Password can be search out through memory dump.

Now perform search for the gmail account and credentials for that account can be easily identified. It is not necessary that the account should be opened in the browser. The detail of the account though the user is not logged on can be extract. If user logged in through private browsing mode, then also the detail about the account can be identified. Full emails and chats with the date and time can also be extract through serching. Investigator also can listed out all the contacts of that account.



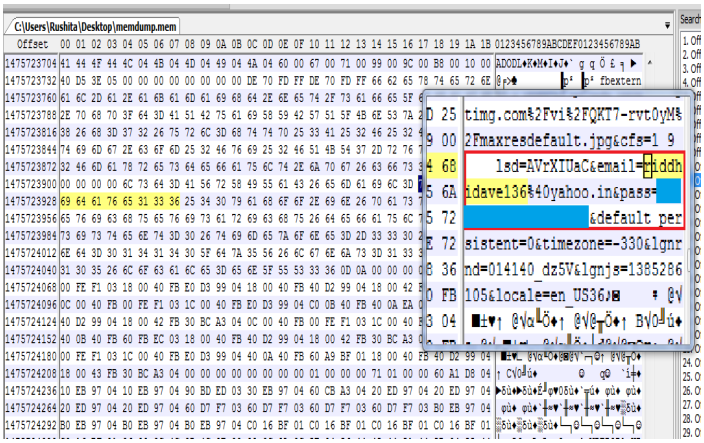
Gmail email content can be seach out through memory dump

Another potential evidence chat conversation of the user is also there in the memory dump.



Chat conversation

Social networking site facebook credentials can also got through Live RAM analysis.



Facebook credentials

VI. CONCLUSION

Volatile memory analysis will be essential to the digital investigation process going forward. While there are many tools existing for live memory acquisition and analysis, it is still a comparatively new attempt in the area of digital forensics. As the tools become better and the actions more sound, analyst will have a new weapon to utilize during forensic investigations. In the future more work can be done on interpretation of RAM data in a human readable form.

VII. REFERENCES

Mubarak Al-Hadadi and Ali AlShidhani, "Smartphone Forensics Analysis: A Case Study", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.

CHANG Xu, TANG Xin-hua, WU Jian, "Forensic research on data recovery of android smartphone", 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013).

Freddie Witherden, "Memory Forensics over the IEEE 1394 Interface".

Vrizlynn L. L. Thing a,*, Kian-Yong Ng b, Ee-Chien Chang b, "Live memory forensics of mobile phones Vrizlynn L.", digital investigation7 (2010) S74eS82.

Liming Cai, Jing Sha ,Wei Qian, "Study on Forensic Analysis of Physical Memory", 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013).

B. D. Carrier and J. Grand, "A Hardware-Based Memory Acquisition Procedure for Digital Investigations" Journal of Digital Investigations, March 2004.

Microsoft, Inc., "Windows feature lets you generate memory dump file by using the keyboard", December 2007, http://support.microsoft.com/kb/244139.

H. Carvey, Windows Forensic Analysis, Burlington, MA: Syngress Publishing, 2007.

AccessData,"Forensic Toolkit 2.0", http://www.accessdata.com/Products/ftk2test.aspx.

AccessData, "http://www.accessdata.com/products/digital-forensics/live-response"

AccessData, "http://www.accessdata.com/services/digital-forensic-services/data-aquisition-preservation"