Live Memory Forensic Analysis

Jyoti Belsare
IT System and Network Security
GTU PG SCHOOL, Gujarat Technological University
Ahmedabad, India
jyoti.belsare@gmail.com

Aditya Sinha
Principal Technical Officer
ACTS and HPCS
Pune, India
saditya@gmail.com

Abstract **-** The live memory image acquired in live forensics is always view in terms of integrity and reliability when presented as evidence. In this work, I describe how evidence like live memory obtained from physical memory image (RAM) and trustworthiness of evidence is studied. The evidence in live memory image can be taken as how accurately the memory image of RAM shows the real memory of the target machine. Based on a live memory analysis, investigator can test memory acquisition tool and after that live memory image is analyzed. Then, I describe the part of live memory analysis in the digital cyber forensics process and its use to address many challenges of the digital forensic investigation. In this work, I provide a method to overcome these problems. I highlight at some of the existing methods to live memory analysis. This work is done using acquisition and analysis tools.

Keywords **-** *Computer Forensic, Physical Memory Forensic, Live Memory Analysis*

*****

I. Introduction

From recent time, an increasing amount of attention has been given to research in the area of live memory forensic analysis. Very few forensic investigators have the time to include live memory (RAM) for the digital investigation purpose. There is also lake of labs, experts, resources and tools for live memory analysis in the digital investigation process. Some of them feel it as it is waste of time for the investigation. For that reason, investigators won't give priority to collect live memory during incidence response phase. The main reason of this work is to highlight that live memory analysis for forensic purpose should not be taken as burden for the digital investigator, but important part of digital investigation process.

There are a lots of significant forensic principles to study when pull out data from live system (RAM). This concerns on trying to reduce the modifications to the system [1]. Small work has been done to calculate how live data is collected can follow to these principles. I will make available some primary awareness into the limits and obtrusiveness of several tools and methods that are typically used for live response and analysis.

A. *Concepts of Windows Physical Memory Analysis*

The digital data collected in current live forensics is always doubted in terms of truthfulness and consistency when observed as evidence. In this work, I determine the part of live memory analysis in the digital investigation process and how that analysis can be used to report many of the challenges of digital forensic investigation process. And the credibility of evidence acquired from live memory image is considered. The reliability of evidence in physical memory image of live memory can be addressed as how carefully the memory image precisely or truly characterizes the real memory of the target machine. Firstly, the conclusion of memory acquisition tool on live forensic evidence is analyzed. Then, this image will be stored in database with particular time stamp at Digital Evidence Collector.

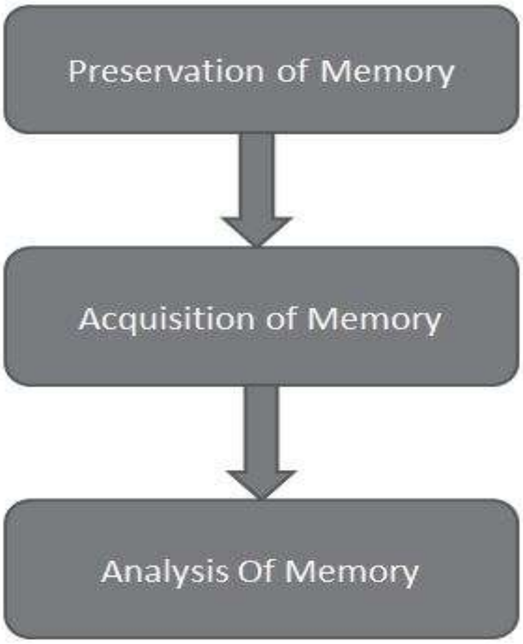


Figure 1. Memory Analysis Steps

B. *Key Technology of windows physical memory analysis*

There are two main aspects for windows physical memory analysis: one is how to get the physical memory, and generate physical memory image files; the other is how to analyze the physical memory image file, and find out the important invasion evidence.

C. *How to acquire physical memory*

1) Methods based on hardware[2]:
   a) Tribble
   b) FireWire
2) Methods based on software[2][3]:
   a) FTK manager
   b) DumpIt

c) Redline
d) Microsoft crash dump

II. Research Methology

There has been a good attention paid to acquisition and analysis of physical memory in the past years. For physical memory acquisition, Sarmoria and Chapin (2005) presented a runtime monitor to log read and write operations in memory-mapped files [3] [4].

For this research, first I have to preserve the evidence. Here, Preservation is the process by which we can make sure that the evidence is un-tampered with and continues to be in the state in which it is found. After preservation, acquisition is conducted. Acquisition is the process of acquiring or gaining the evidence. Various hardware-based and software-based tools have been recently developed for memory acquisition. And after acquisition, I can analyze this evidence. Analysis is the process of going through and discovering what type of information and evidence that we have acquired. There are some tools for analyze the memory like FTK Imager, COFEE, EnCase, etc.

A. Acquire Memory

By using this tool we can:

- Acquire the physical memory in raw image using multiple methods, and preserve this image in device.
- Convert this raw memory "image" to Microsoft crash dump format so that the resulting data can be analyzed using the Microsoft Debugging Tools [7].
- Acquire to a local removable (USB, FireWire) storage device as well as via the network using TCP/IP
- Designed specifically for forensic use, with audit logging and cryptographic integrity checks

B. Anlysis of Memory

Going through and discovering what type of information and evidence that we live memory analysis, investigator analyzes RAM memory. RAM contains different type of data and these data can be modified at any time.

Different types of data have acquired in RAM:

1) System time
2) Logged on user
3) Open filesNetwork information
4) Process information
5) Process-to-port mapping
6) Process memory
7) Service/driver information
8) Command history

Next step after the analysis process is to find out relative information from memory. This can be done by answering some question like:

1) What hidden processes were running on the system, and how were they hidden?
2) What other evidence of the intrusion can be extracted from the memory dumps?
3) What computer was the intrusion launched from?
4) Is there any indication of who the intruder might be?

III. Proposed Method

In this work, I show the important role of live memory analysis in the digital investigation process and its use to provide solutions for many problems that faced by the digital forensics investigation process.

I describe some of the existing approaches to live response in digital forensic investigation. There are number of important forensic principles to consider when extracting data from a live system. These considerations focus on trying to reduce the changes to the system, understanding the effects of the changes, and minimizing the trust that is placed in the system. [11]

Small work has been done to evaluate how good existing methods in live data collection follow to these principles. I will provide some initial insight into the limitations and trustworthiness of different tools and methods that are normally used for live response. I will also introduce FTK Imager, DumpIt, Redline, a toolkit for windows operating system that will allow digital investigator to extract useful information that is available on live system, i.e. take image of raw data of RAM.

A. Process Flow for Gaining/Analysing Live Memory

1) Preservation

   Making sure the system, i.e. evidence is un-tempered with and continues to be in the state in which it is found. It is difficult to preserve live memory because it can be modified with time.

2) Acquisition

   The process of acquire or gaining the evidence. This process includes taking image of RAM using FTK toolkit. Back up of this image file must be taken for any future use.

3) Analysis

   Going through and discovering what type of information and evidence that we have acquired. Find related information from image using tools and techniques like which process is running and which IP Address and port is used for connection.

4) Discovery

   Breaking down the acquired evidence and isolating what is called relevant or interesting evidence. In this process, investigator finds relevant evidence from collected information from the crime scene or incident scene. This can be useful to find out the attacker and purpose of the attack.

B. Memory Analysis

1) Identifying Context
   - *a)* Find the Kernel Processer Control Region (KPCR)
2) Parse Memory Structures
   - *a)* Executive Processes (_EProcess) blocks
   - *b)* Process Environment Blocks (PEB)
   - *c)* Tracks DLLs loaded
   - *d)* List of process memory sections
   - *e)* Kernel modules

f) Drivers

3) Scan for Outliers

a) Unlinked Processes, DLLs, sockets and threads

b) Unmapped pages with execute privileges

In proposed method, there are various steps to collect live memory image from running device. With this method, investigator can make sure that he/she will get raw image of live memory at every time stamp and stored in database. So, this database is used later to analyze live memory and also used to collect evidence of wrong doing which can be used to present in law of court.

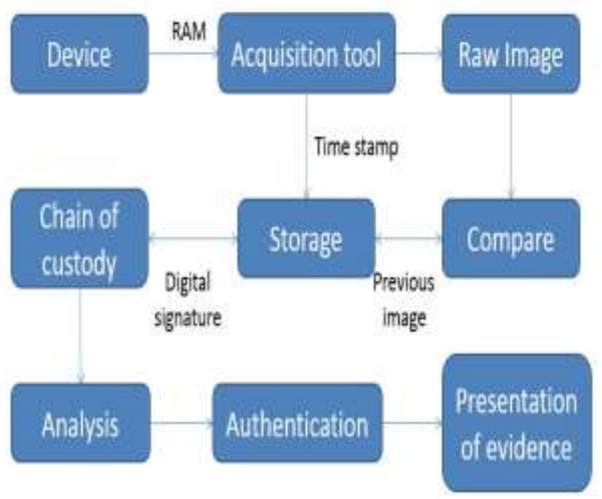


Figure 2. Process flow of collecting live memory image

There are following steps for this method:

1) Identify available sources and different types of potential evidence. This includes running devices and also not running devices. Keep all devices in the state in which they are found.

2) Now, for running device investigator has to collect RAM image for discover useful evidence. It can be collect using FTK Imager.

3) After that, FTK start copying live memory into raw image bit by bit. This raw image then stored into storage database called digital evidence collector. In this database, time stamp and digital signature is also included for authentication purpose.

4) Then after this process is repeated and generate another image with second time stamp.

5) Now this both image is compare and only changed bits are stored in database with second time stamp. And this whole process is repeated for every time stamps in storage.

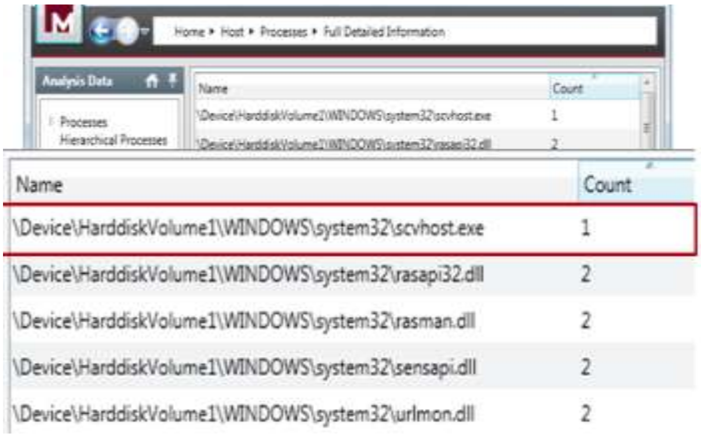
6) Now for analysis process this image is used. So there is possibility of compromising integrity of this evidence item. To prevent this situation, various backups can be taken and stored. Also chain of custody document is prepared to keep track of persons who analyze this evidence.

7) After all this process, authentication is done to verify all the process. By authentication process, investigator can verify that evidence is inacceptable stage and chain of custody document make sure that only authenticate person accessed the evidence.

8) So that this evidence is applicable in law of court procedure.

IV. Discovery of Evidence After Analysis

By using Redline analysis tool, I find many malicious process. Like, the correct spelling should be sVChost.exe NOT sCVhost.exe. The correct svchost.exe should occur more than one time on a windows system.

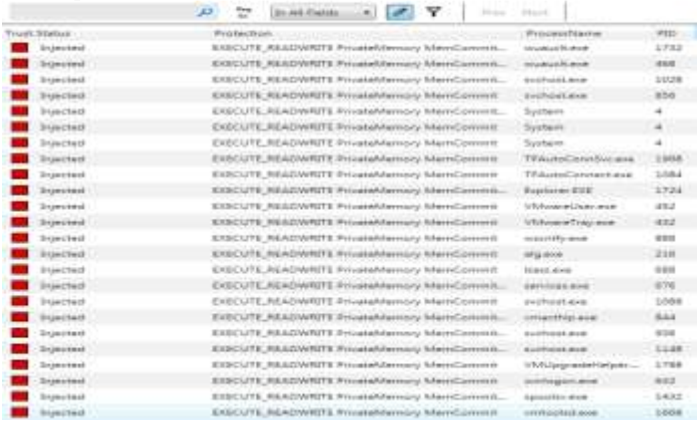


Name	Count
\Device\HarddiskVolume2\WINDOWS\system32\scvhost.exe	1
\Device\HarddiskVolume1\WINDOWS\system32\rasapi32.dll	2

Name	Count
\Device\HarddiskVolume1\WINDOWS\system32\scvhost.exe	1
\Device\HarddiskVolume1\WINDOWS\system32\rasapi32.dll	2
\Device\HarddiskVolume1\WINDOWS\system32\rasman.dll	2
\Device\HarddiskVolume1\WINDOWS\system32\sensapi.dll	2
\Device\HarddiskVolume1\WINDOWS\system32\urlmon.dll	2

Figure 3. Malicious process

It gives you the ability to quickly triage memory processes. The below process indicates that the "Process has a known mutant for "sobig" malware". Using Redline's Malware Risk Index (MRI) hits, you are able to quickly tell that this is a malicious process.



Trust Status	Protection	ProcessName	PID
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	wuauclt.exe	1732
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	wuauclt.exe	468
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	svchost.exe	1028
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	svchost.exe	856
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	System	4
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	System	4
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	System	4
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	TPAutoConnSvc.exe	1908
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	TPAutoConnect.exe	1084
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	Explorer.EXE	1724
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	VMwareUser.exe	452
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	VMwareTray.exe	432
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	wscntfy.exe	888
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	alg.exe	218
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	lsass.exe	688
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	services.exe	676
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	svchost.exe	1068
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	[illegible]	644
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	svchost.exe	936
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	svchost.exe	1128
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	VMUpgradeHelper...	1788
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	winlogon.exe	652
Injected	EXECUTE_READWRITE PrivateMemory MemCommit...	spoolsv.exe	1432
Injected	EXECUTE_READWRITE PrivateMemory MemCommit	vmtoolsd.exe	1608

Figure 4. A few processes that indicate DLL Injection

Figure 5. Malware Risk Index (MRI)

V. Conclusion

For collecting live memory image, many tools are available to discover valuable evidence from the live memory image. With hardware method to acquire the system live memory is an ultimate key, as it has simply no effect on the system live memory, won't terminate or replace the information in live memory, and can acquire whole memory. We have some software tools to acquire the system live memory, but using this tools will unavoidably terminate even replace the data and information in live memory.

Since there is no algorithm developed on described solution. There are various tools available for extracting live memory image. Also there are different methods to store this image. But there is no such tool that can verify the integrity of this image. I proposed the solution for this problem. With previously described method investigator can make that extracted image is authenticated and acceptable in law court. So I am looking forward to implement algorithm for given solution.

References

[1] AAron Walters, Nick L. Patroni, Jr., "Integrating Volatile Memory Forensics into the Digital Investigation Process"

[2] Lianfu Yin, "Research on Windows Physical Memory Forensic Analysis", 2012 Fourth International Symposium on Information Science and Engineering

[3] Sarmoria CG, Chapin SJ. Monitoring access to shared memory mappedfiles. Digital Forensic Research Workshop (DFRWS),2005

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

[5] Lianhai Wang, Ruichao Zhang, Shuhui Zhang,"A Model of Computer Live Forensics Based on Physical Memory Analysis", The 1st International Conference on Information Science and Engineering (ICISE2009)

[6] AmerAljaedi, Dale Lindskog, PavolZavarsky, Ron Ruhl, Fares Almari,"Comparative Analysis of Volatile Memory Forensics - Live Response vs. Memory Imaging", 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing

[7] Gabriela Limon Garcia, "Forensic physical memory analysis: an overview of tools and techniques"

[8] GCFA Gold Certification, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory"

[9] Guidance Software. EnCase forensic. Retrievedfrom:http://www.guidancesoftware.com/products/ef_index.asp.

[10] Microsoft Corporation. Windows Hardware Developer Central. Memory Management: What Every Driver Writer Needs to Know. Retrieved from: http://www.microsoft.com/whdc/driver/kernel/mem-mgmt.mspxFebruary 2005. On January, 2009.

[11] https://www.blackhat.com/presentations/bh-dc-07/Walters/paper/bh-dc-07-Walters-WP.pdf