

TECHNICAL ISSUES & CHALLENGES IN MEMORY FORENSICS

¹Prathamesh Kapade, ²Dr. Atul Kumar Pandey

¹STUDENT, ²HOD

¹RGNCLC,

¹NLIU, Bhopal, India

Abstract : The online medium has evolved to be an attractive platform for committing frauds, as it offers better returns than the usual methods. The use of various hacking tools has made it even easier for anyone to implement. In such a scenario it becomes difficult for investigative agencies to collect concrete evidences which can be vital to prove crime against the cyber criminals in the court of law. The evidence collected from the primary memory can be crucial to prove the facts, as it depicts the live data and is not easily modified. Given this, it is essential to examine the technical issues and challenges posed by the memory forensics.

IndexTerms - Cache Memory, Cyber-Crime, Digital Evidence, Electronic Evidence, Memory Forensics, Legal Issues.

I. INTRODUCTION

This paper identifies major issues and challenges in memory forensics and is based on theoretical concepts and practical implementation of memory forensics. The present day technology allows us to perform memory forensics, on both volatile and non-volatile memory, which aids in cyber-crime investigation among other purposes. In order for it to be identified as digital evidence the confidentiality, integrity and availability of it must be preserved so that assurance can be provided that the evidence collected from memory is not tampered and qualifies to be admissible in the court of law.

The memory analysis is done using a number of tools which are either proprietary or open source. As the proprietary tools are expensive, most of the security researchers use open source tools to perform memory forensics. These tools can be very effective in performing memory analysis can also help in performing malware analysis specifically those that reside in main memory which are referred as memory resident malware. The specialty of these malware is that they have the ability to attach themselves with the system process making it difficult for the antiviruses to recognize. The memory forensics tools allows us to perform deep analysis of the running processes, attached DDL files and recognizes the malicious or suspected signatures (like the MZ signature) of the malwares.

The memory forensics presents significant challenges throughout the process such as it requires a high level understanding of the technology and the underlying architecture of the system in order to perform it. There are such professionals who perform it but among them the best one's are those who can develop their own tools using any scripting language. The related work explained in the next section focuses on the main memory, while this research work is focused more on technical issues and challenges posed by the memory forensics and proposes a solution for it.

II. RELATED WORK

There is significant amount of research work available, but most of them are focused on primary memory forensics implemented using open source tools like volatility. Other researchers have also contributed in malware analysis, for which the data was extracted from the primary memory using volatility, where the extraction is done either by creating the image or by creating the memory dump file. Some researchers have also focused over the integrity of the acquisition made and have devised certain methods to measure the correctness of the acquisition file. The author's perspective is focused on the technical issues & challenges in memory forensics which may pose difficulty in forensic investigation.

III. TECHNICAL ISSUES IN MEMORY FORENSICS

The memory forensics is a core technical concept and may face some technical issues in its implementation process and its extension methods. In situations where the data is collected from the main memory of a system, it is imperative to maintain its integrity and it should not be exposed to modification before and after its analysis. The same applies to the data recovered from the secondary memory.

Issue: Modification by Malware

Description: In the beginning of the computer era we did noticed the adverse effects of computer program to which we call a virus. Further, many upgraded and new versions of such programs were witnessed well known as Trojans and Malwares. All of these can collectively be called as threat agents. These threat agents have the capability to modify the data without the knowledge of the user. This is common scenario with the secondary memory, but in recent times these malware have evolved and have developed the ability to modify the live data within the volatile memory, specifically RAM without being detected. These malwares are also known as memory resident malwares and are capable of playing with the live data. However, only a skilled person can detect these malwares through malware analysis but then the data collected for analysis cannot be trusted. Besides, every time before analyzing the data from RAM and HDD (Hard Disk Drive), the analyst has to make sure that the data collected from RAM and HDD does not contain any malware. Usually such malware are well programmed to hide by attaching themselves to any system process. Malwares with such ability can cause huge impacts and thus create a significant technical glitch with both volatile & non-volatile memory forensics.

Issue: Deadlock

Description: There are certain times when there are too many processes executing in the RAM exceeding its limits, which may cause a possibility of Deadlock (A condition when the system is hanged up due to overload) in the system. Performing acquisition during a deadlock may result in inconsistent data being acquired. The deadlock is a state where a process requests a resource from the CPU and that process is already being used by a different process for its execution eventually resulting in a cyclic error where each process awaits for the resource to be freed by another process. In such a situation no progress is made and the system should be restarted to resume the processes. Although this could also be a solution for memory acquisition when performed manually which is explained in the conclusive part.

Issue: Page Fault

Description: The page fault is a type of interrupt which is raised by the hardware when the running programs in the main memory attempts to access a memory page which mapped to virtual address space but not loaded in the physical memory. The page fault may happen anytime as it is a circumstantial event. However, each page fault requires transferring data from secondary memory to primary memory and this process may only take a few milliseconds to complete, but still can be several thousand times slower than accessing data directly from the memory.

The page faults may create problems while acquiring memory from RAM, it may also result in smearing. With respect to memory forensics the researcher has identified two such cases where it is possible, they are:

- Acquisition during a page fault may result in acquiring incomplete or corrupted data.
- There may arise a situation where there is a forced page fault. This can happen when a malware is active in the main memory and submitting false page requests to the OS. This will force the OS to look for that specific page in the virtual memory thereby consuming resources unnecessarily. Acquisition during this period will again result in incomplete, corrupted or irrelevant data.

Issue: Forensics in IoT Devices

Description: As of now only a handful of categorized devices were able to connect to the internet. But with introduction of IoT the range of such devices (devices with internet access) has widen to include home appliances, electronic devices etc. In order to provide ease of access to these devices, which was not the case earlier as it was a physical operation, all are connected to internet and can be accessed through an application for management purposes. Given the small size of IoT devices, there isn't much scope for the security of these devices making them vulnerable and easy target for hackers. There have been reports, that the IoT devices were used to execute the DDos attack, which brings them in the vicinity of forensics.

With reference to the research topic, the major issues with the IoT devices is the problem of acquisition. This problem arises mostly in cases where commercial IoT devices are deployed. Due to its strict requirements they have very small storage and provide only specific functionalities and also have limited accessibility options. Due to which it becomes extremely difficult to access the devices firmware/OS and acquire the memory dump or image of both primary and secondary devices.

For research purpose the researcher experimented with the cost effective product Raspberry Pi 3. It has the OS built in known as the Raspberry Linux and acquired the dump using "dd" command from the /dev/mem facility. Following are screen shots of both:

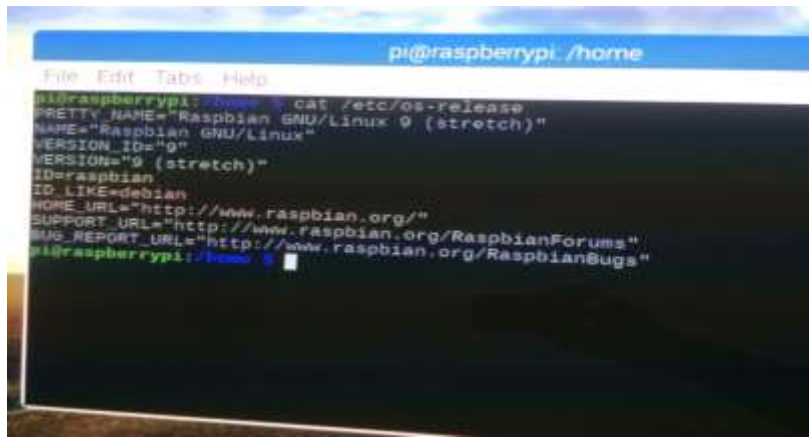


Figure 1: Depicting the raspberry OS release.



Figure 2: Depicting the “dd” command.

The above screen shots make it clear that it has a Debian based kernel specially built for the Raspberry Pi. The device is equipped with 1Gb of primary memory of which the dump acquired was found to be corrupted and therefore could not be analyzed. The tool used for this was ReCALL Memory Forensics tools.

There are many commercial IoT products available in the market. For example, one such low cost product, known as Oakter, was considered which is IoT enabled and is used to manage the electronic equipment’s like lights, fan, power plug etc. The product has one server like machine which is the central system deployed at the site connected to a cloud server and is used to manage the clients like power socket, lights etc. This system doesn’t have any means to connect except the mobile application. It doesn’t even have any USB ports. Due to such limited accessibility it becomes difficult to acquire the memory dump.

As the number of cyber incidents using IoT devices are increasing it is imperative to perform memory forensics on the IoT devices. For this purpose the hardware manufacturers must make an amendment to their policy or designs which could favor forensics in IoT devices.

IV. TECHNICAL CHALLENGES IN MEMORY FORENSICS

Most of the challenges in memory forensics arise from the issues which are discussed in the previous section. Solution of every issue is itself a challenge and needs to be resolved so that integrity of the evidence can be maintained. Following are the challenges identified within the scope of this research:

Challenge: Memory Acquisition During Deadlock.

Description: Memory acquisition is itself a challenge pertaining to memory forensics. Given the identified issues in memory forensics, acquisition during a deadlock should not be attempted as the processor is already over-occupied, opening another process at that instant may force the system to a crash thereby destroying all the possible evidence within the main memory. Therefore the

investigator must wait for the system to end the deadlock. Alternatively, an even greater challenge for the investigator is to force the system out of the deadlock situation.

Challenge: Memory Acquisition from IoT Devices.

Description: A prospective challenge posed by the IoT devices is for the manufacturers to provide a hardware based approach to access the device so that the memory can be acquired. This is a part of research in the development of IoT devices. As the cyber-attack frequency is increasing using the IoT devices, it will become imperative to perform forensics on these devices and therefore the OEM's will have to provide a way of doing it.

Challenge: Maintaining the Integrity of Data.

Description: Another prospective challenge in memory forensics arises from the fact that makes it possible to compromise the integrity of the data collected from the RAM and HDD. Given this, another kind of memory source must be used, either in addition or combination, which is present within the system in its physical form, and which can potentially play a vital role to strengthen the evidence collected from memory forensic. For such a purpose cache memory should be used to cross verify the evidence of live memory forensics.

Challenge: Data Encryption within RAM.

Description: This challenge is basically a proposed solution so that unauthorized modification by the malwares within the main memory can be stopped. The data which resides in RAM is volatile in nature and no longer exists when the system is powered off. During the powered on state the data in main memory should be encrypted to avoid any modification by a malwares. This can be achieved, if the OEM's can develop a hybrid RAM which has a specific section to store non-volatile data within the RAM. This new section should be used to store algorithms which will perform the encryption. So, practically whenever a new process is loaded in RAM all of its content will be encrypted first and then the execution.

Such a concept will definitely have side effects such as it will slow down the speed of the system but will provide higher degree of security.

Another thing is that the decryption keys should rest with an authorized body and be made available as per the policies. One such example of policy would be, that the keys will be given to the investigative agencies authorized by law to perform memory forensics.

Challenge: Data Extraction from Cache Memory.

Introduction to Cache Memory: In order to investigate a cyber-crime, system cache memory analysis may play a vital role in identifying some more evidences from the cache. The cache memory is the fastest memory present in a computer system which can be found installed at three different levels named as L1, L2 & L3 cache respectively. L1 is the fastest in speed and compact in capacity followed by L2, and L3 being the one large in size compared to other two. L3 being the slowest in cache but is still faster than primary memory. The purpose fulfilled by the cache memory is to provide faster access to data required by the processor.

The cache memory holds the information which is frequently accessed by the processor to complete the tasks at hand. This information could be anything starting from text files, images, multimedia files to OS internal information. More information can be extracted from the L3 cache as it is a high capacity cache among all three.

Among the three of them, the L1 cache is integrated in the processor thereby referred as internal cache. L2 and L3 are referred as external cache. In recent years the L1 and L2 both are integrated within CPU leaving L3 as the only external cache. For the purpose of this research, the word Cache Memory refers to the memory installed in its physical form in the system and not to be confused with other cache like browser cache or application cache.

Challenge Description: The cache memory as described is a volatile memory used by the processor to store data frequently accessed by the CPU increasing the overall performance of the system. At times it is possible that all three levels of cache may hold different set of data. If extracted, this data may support the overall memory forensics, as till date it cannot be modified not even with the help of a memory resident malware. However, subject to certain conditions, the cache memory can also be corrupted. Two such conditions identified by the researcher are as follows:

- The cache memory fetches all the data from the main memory and if the malware is present the main memory it may send corrupted data to the cache.
- Second condition would be if the data is corrupted within the secondary memory or the non-volatile storage, which is requested by the processor.

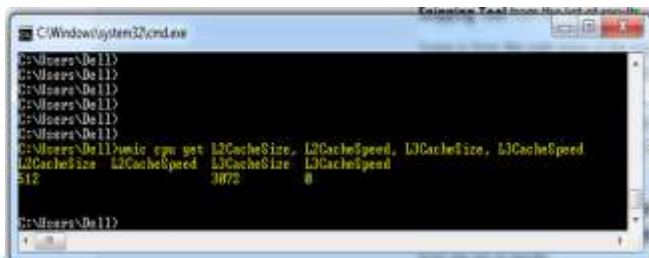
But the challenging task with the cache memory is to extract data from it. As of now there is no such defined approach to access and save the live data from the cache. Although, operating system provides the utility which helps us to check the details regarding cache.

Windows operating system uses one such utility called “wmic” which displays the information regarding cache memory. Consider the fact that the information provided by this utility is of the system cache memory and not of any application. On executing the following command it will display all the information except speed of the cache memory:

```
“wmic memcache get /ALL”
```

The output of the command specifies the measures like purpose, size, max size, blocks etc. for all the cache levels. Following is one more command in windows which displays very specific values related to cache memory:

```
wmic cpu get L2CacheSize, L2CacheSpeed, L3CacheSize, L3CacheSpeed
```



```
C:\Users\De113> wmic cpu get L2CacheSize, L2CacheSpeed, L3CacheSize, L3CacheSpeed
L2CacheSize L2CacheSpeed L3CacheSize L3CacheSpeed
512          3875          0          #
C:\Users\De113>
```

Figure 3: Depicting the wmic command output.

Further upon requesting the L1 cache details the system returns “Invalid query”.

Another challenge in the cache memory forensics is the power. Due to the volatile nature of the cache memory one has to fetch data from it when its powered on, once the power is off all the information in it will be lost.

Importance of Cache Memory: Cache memory is an integral part of the processor and works closely with the processor. Normally, when a resource is requested frequently it is stored in the cache for providing faster access to it. For cache RAM acts as the bridge between cache and secondary memory. In this chain of assistance it would not be incorrect to call RAM as the L4 cache.

In current scenario the cyber forensic domain has been restricted to the primary (RAM) and secondary (HDD) memory forensic, from where maximum possible information can be extracted due to its large size, and when combined with the timestamp it becomes the accurate information required. In order to increase the granularity of the evidence collected from the RAM of a system it is best to synchronize and combine it with the evidence collected from the cache memory which will eventually make it more concrete. This is necessary as the data collected from any memory except cache can be modified compromising the integrity of evidence.

VII. CONCLUSION & SUGGESTION

The technical issues and challenges listed in this paper are presented with respect to memory forensics and address the technical problems associated with memory forensics. The technical problems are more specific to the available operational analysis of the RAM and operating system. Even though this research proposes the idea of encrypting the data within RAM to maintain the confidentiality and integrity of the data there is a possibility idea of using cache memory and also including it in the memory forensic process which may help in making the digital evidence more concrete.

The technical issues mentioned in the paper can be resolved by taking appropriate measures such as encryption, proper scheduling of process etc. so that the malware and deadlock situation can be separated from the memory forensics. However, the challenge of collecting the data from cache still remains which the researcher would like to reserve as future aspect of this research.

The researchers propose the idea of developing the operating system in such manner so as to separate the kernel and application execution space within RAM eventually making the acquisition process much simpler. This will also reduce the amount of data acquired saving storage space and also the time required for examination and analysis. Also the tools used must have options to acquire the specific memory for analysis.

REFERENCES

- [1] Andrew Case, Golden G Richard III, Memory Forensics: The Path Forward, Available At - https://ac.els-cdn.com/S1742287616301529/1-s2.0-S1742287616301529-main.pdf?_tid=e5e6f761-05ad-4e65-a0dc-c2b063a05cef&acdnat=1522148579_7f2562920effdedd3c719a169cb67780, Last Accessed on 27/03/2018
- [2] James Butler and Justin Murdock, Physical Memory Forensics for Files and Cache, Available at - https://media.blackhat.com/bh-us-11/Butler/BH_US_11_ButlerMurdock_Physical_Memory_Forensics-WP.pdf, Last Accessed on 31/10/2017