LEGAL ISSUES & CHALLENGES IN MEMORY FORENSICS

[1]Prathamesh Kapade, [2]Dr. Atul Kumar Pandey
[1]STUDENT, [2]HOD
[1]RGNCLC,
[1]NLIU, Bhopal, India

Abstract: In the past decade the online medium has evolved to be an attractive platform as a market place for making purchases of almost any commodity and 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 the absence of approved guidelines for collection, acquisition and preservation of electronic evidences (herein after referred as EE) with respect to memory forensics (herein after referred as MF), 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. Given this, it is essential to examine the legal issues and challenges posed by the memory forensics.

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

I. Introduction

With the evolution of "Ease of Access" concept everything has become available over the domain of internet. As the number of customers has increased exponentially, resulting in a large amount of money being involved and also providing more space to commit a crime. There have been cases of online frauds being committed by the malicious individuals and they were able to escape it just because they cleared their tracks to become untraceable. This has become a practice among hackers to avoid being detected.

In India, in certain cases it has been observed that after committing a cyber-crime criminal escapes the charges framed under the IT Act, 2000 just because the opposing party were not able to prove them (Such a scenario was observed in the recent judgement, Jagdeo Singh vs. The State and Ors, pronounced by Hon'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B of the Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever)[1], although the police may book them under other available legal provisions such as the IPC. This happens in most of the cases as the cyber police lacks the necessary qualification and ability to identify a possible source of evidence and prove it. Besides, most of the times the electronic evidence is challenged in the court due to its integrity.

It is also said that the legal framework opts for a soft approach towards criminals and every crimes has to be proved beyond any reasonable doubt, it is only then the punishment is awarded. In order to prove a crime beyond reasonable doubt evidence plays the most vital role. With respect to cyber-crime and its subdomains, such as memory forensics which is also the subject matter of this research, evidence is challenged by questioning its integrity. It also becomes easier to challenge the evidence as there is an absence of clear guidelines for collection, acquisition and preservation which are approved by law, with respect to electronic evidence. In the absence of such guidelines and not being able to prove the process of collection/acquisition of an electronic evidence (referred as EE herein after) the evidence itself gets discarded. This research work presents such legal issues and challenges presented by the memory forensics and propose a solution for it.

II. Related Work

So far, the researcher has not come across any significant and relevant research work in the domain of memory forensics addressing the legal issues and challenges. This research work is focused towards addressing the legal issues and challenges of memory forensics and considers the country specific scenario with respect to the Republic of India.

III. Legal Issues in Memory Forensics

There are many instances where the legal framework requires a soft approach and does not recognizes all of the subdomains of the cyber-forensics. The MF is one such subdomain and presents significant issues in its implementation and recognition of evidence. All such identified issues are as follows:

[1] http://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf

Issue: Absence of clear collection/acquisition guidelines.

Description: The process of memory forensics (referred as MF herein after) begins with the knowledge of the state of the system. The state of the system under investigation determines the choice between two processes collection and acquisition. There is a difference between collection and acquisition processes. The collection is performed when the system is in the OFF state, that is powered off, so that it can be collected in its physical form and be taken to the lab for further analysis. And the acquisition is performed when the system is powered on. In the process of acquisition the investigator will collect all the virtual artifacts present in the hard disk drive (to be referred as HDD herein after) and random access memory (to be referred as RAM herein after). However, the acquisition of the virtual artifacts is tricky and requires extreme caution, any unjustified mistake at this stage will result in the evidence being challenged. The issue is the absence of guidelines approved by law to perform the acquisition and collection. In such absence the investigators have justify the whole process of investigation, which has a high possibility being challenged, in the court of law.

Issue: Absence of clear preservation guidelines.

Description: In cyber forensics the investigator never performs the forensics on the original piece of source of evidence (as part of best practices followed), they make a copy of it and then the forensics is performed on the secondary. With respect to MF once the MF has been performed the investigator will list out all the findings and then the investigator has to preserve the possible primary evidence in order to present it in the court of law. As of now, no such preservation guidelines have been approved by the law which could be followed further down the line. The importance of the preservation guidelines stems from the fact that the cases in India may live up to many years. Some of the cases did lived up to 20 years, which is a challenge explained in further sections.

Issue: Limitation of the Indian Evidence Act.

Description: After the amendment in 2000, the Indian Evidence Act (referred as IEA, 1872 herein after) started to recognize the EE as the documentary evidence and also it became admissible in the court of law. For the admissibility of electronic record section 65B was inserted in the Evidence Act to address the admissibility problems with respect to the EE. Although there are issues which arise out of the limitation of the Evidence Act, as it is not able to evolve with time and address the EE admissibility problems of evolving technology due to many ways such as the EE are more susceptible to tampering, alteration, transposition, excising, etc. The Act and this section are silent on the ways to perform memory forensics and do not even specify guidelines to perform it instead the Act does specify that any EE being presented in the court must accompany a certificate as per section 65B sub-section 4. This means no matter what procedure is followed it must be proved with the help of a certificate. This Act should at least prescribe the procedure or standards to be followed to perform MF just as IT Act, 2000 prescribes wherever necessary.

Issue: Size of the Electronic Evidence.

Description: With respect to memory forensics, the size of the evidences acquired from the memory is very large as compared to other EE. Whenever MF is performed for the purpose of gathering evidences from the memory, the investigator has to create the image of the memory and then examine the image itself and not the original source of evidence. This image being created is of the size of the disk. For example, if the investigator is creating image of an HDD of size 1TB then the output image will be of size 1TB irrespective of the size of data present in it. This process consumes more time and unnecessary storage space.

IV. Legal Challenges in Memory Forensics

As stated in previous section, memory forensics has many issues which are no less than a hurdle in proving a fact using the evidence collected from the memory. Not only the issues with MF, it also presents significant legal challenges which needs to be resolved for effective implementation to resolve the cyber-crimes. The researcher has identified a few legal challenges posed by the MF, they are:

Challenge: Preservation of EE.

Description: In cases where the EE could be admissible, an issue which is addresses the preservation guidelines uncovers the fact that preserving an EE, which may involve a technical process, is itself a challenge as there are instances where a case law lived up for more than 20 years. Practically, preserving an EE for more than 20 years in not possible as within that span of time the technology may evolve many folds. It is possible that preserving that long will require a lot of money to maintain the state/form of the EE and the technology which could be used with that EE.

Challenge: Regular update of Legal Framework

Description: In the Indian scenario, the law making process has a gradual approach and therefore it may take long time for a law to get enforced after it has been passed in the Parliament. In a view, this approach is effective as the draft passes through many evaluations before it is presented in the Parliament. Due to this stringent approach, if a researcher finds a flaw within the law itself, it

is rectified in the next amendment of that law, until then it is the Honorary Supreme Court of India which pronounces such law either obsolete or gives a relevant interpretation of that law.
All this process is time taking and may take years. As for MF and the technology used in this domain, it is essential to regularly update the legal framework as the new technologies are being developed which can be used to execute a cyber-crime. In future if this challenge is met and resolved, it will also address the issue of limitation of the IEA,1872.

Challenge: Examination of Large Size EE.

Description: This challenge arises from the issue of size of EE. As the size gets larger it may complicate and make the evidence extraction process a tedious task. Wherever the EE extracted from the acquired image contains text files (with extension .txt, .pdf, .doc etc.) it will consume more time to analyse as the text documents as large as 15 MB may contain more than 50 pages for analysis. If the evidence is in the form of image then the investigator must establish that the image is not a tampered one. Another case can be considered that of any media file which can be of more than 1 GB and to analyze such a big file takes time. The examining tools are not that smart as of yet to reduce the time of examination and analysis which eventually results in delay of court hearings.

V. Collection / Acquisition Guidelines

With respect to the Indian scenario, there are no adequate collection and acquisition guidelines, which are approved by law, and are available which could be enforced by the investigative agencies for forensics purpose. For this purpose the researcher proposes the guidelines for collection and acquisition of EE. While collecting EE some factors need to be considered such as the state of the system and whether to perform acquisition or collection. All the task is to be performed by an Authorized Investigator (referred as AIG herein after). Practically all the four combinations are possible with a little bit of dependency on each other.

Collection Guidelines: Collection of EE majorly refers to the gathering of EE in its physical form. The collection can be performed in two states of the system that is powered on and powered off.

Status: Powered On: If the status is powered on following steps should be followed for collection of EE:
1) Once confirmed state is on, the AIG must check if the volatile data required from the system.
2) If YES in STEP 1, acquisition guidelines must be followed where the state of the system is “powered on”.
3) If NO in STEP 1, then the AIG must initiate normal shutdown process of the system.
4) The AIG must label the system, peripheral devices, cables etc. and tape the power plug of the system.
5) The collection process is completed and the collected systems can be seized as per the law.

Status: Powered Off: If the system status is powered off following steps must be followed for collection of EE:
1) The AIG must check if the system relies on battery. If YES, then the AIG must do the following:
a) Remove the battery.
b) If possible, remove the secondary storage media.
c) Label the storage media and document all the details of storage media, and the actions committed so that chain of custody can also be maintained.
If NO, the AIG must remove the power directly from the system.
2) The AIG must label all the hardware and peripheral devices, cables etc. and also place a tape over the power plug of the system.

Acquisition Guidelines: The acquisition of EE refers to gathering of EE from the volatile and non-volatile memory. It is performed with extreme caution as any mistake may damage the EE. The acquisition of EE can also be performed in two states of the system, that is, powered on and powered off.

Status: Powered On: If the system is powered on following steps must be followed for acquisition of EE:
1) The AIG must check if the live data is required from the system. If NO then AIG must follow the below mentioned steps:
a) The AIG must check if the system can be seized or not.
aa) If YES then the collection guidelines for powered on systems must be followed.
ab) If NO then, the AIG can stop the acquisition process.
2) If YES in step 1, then the AIG must follow below mentioned steps:
2a) Then AIG must check whether the disk is encrypted. If NO, then proceed to step 3.
2b) If YES then AIG must perform live acquisition of volatile data using appropriate tools and then proceed to step 3.
3) The AIG must check whether live acquisition of non-volatile data is required or not.
3a) If YES, the AIG must perform live acquisition of non-volatile data from the running system.
3b) If NO, the AIG must seal the acquired data, if any, and follow the step 1(a).

Status: Powered Off: If the system is powered off, following steps must be followed by AIG to perform acquisition of EE:
1) Remove storage media from the system.

2) Prepare the target disk for acquisition process.
3) Perform the acquisition, through imaging process, of storage disk into target disk using preferred tools.
4) Seal the target disk.

VI. Preservation Guidelines

Being practical, the preservation phase starts from the very beginning where the possible source of EE is identified and the investigation team must act with care so that the EE is not harmed in any way possible. However, once the collection/acquisition phase is finished the AIG must begin the preservation of the seized possible source of evidence, as it is imperative to keep the EE until the very end or until the case is decided. For such a purpose the AIG must follow the below mentioned steps:

1) Before preservation starts the AIG must make an image of the EE so as not to perform any examination over the original EE.
2) The AIG must use a verification technology such as creating the hash of the source so that any modification attempt can be easily detected.
3) The EE must be kept in a safe place, packed in an anti-static bag which ensures that there is no electrostatic discharge, anti-inflated packing bag or cushion foam to make sure there is no physical damage and making it available as and when required by the legal bodies.

VII. Conclusion & Suggestion

The purpose of this research was to identify the present legal issues and challenges with respect to memory forensics. The researcher identified certain issues and challenges and has proposed a possible solution for most of it by proposing the guidelines for collection, acquisition and preservation of EE. Although there are certain issues and challenges which can be resolved only by the appropriate legislative body.

In cases where the preservation of EE is a challenge, the authoritative legal body should consider the challenge and draft a policy where the courts addressing the cases of EE may record the evidence or store the report of EE examination (either in printed or electronic form), and the preservation of EE for more than 5 years should not be allowed, due to technology evolution the current technology itself becomes obsolete after 5 years.

The IEA Act, 1872 should not use specific terms with respect to technology, such as optical or magnetic media used in section 65B sub-section 1, instead it should use the term “storage media” as in future there may come a new technology which may be different than the present.

.

References

[1] http://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf

[2] ISO 27037:2012, Information Technology-Security Techniques- Guidelines for Collection, Acquisition and Preservation of Digital Evidence