Volatile Memory Forensics: A Legal Perspective

Harnoor Kaur Mann
Cognesol Pvt. Ltd.
SAS Nagar, Punjab
India

Gurpal Singh Chhabra
Thapar University, Patiala,
Punjab, India

ABSTRACT
In today's world of fast changing technology where everything is governed by Internet directly or indirectly, the trend of crime has undergone a dramatic change over the past few years. Today, one can commit a crime with just a click of a button on laptop or computer and enjoy the garb of anonymity and impunity to a great extent. In such a scenario, it has become imperative to throw some light on the emerging issue of tackling cybercrimes in 21st century. This paper describes the extraction and analysis of volatile data that is available in computer's RAM that is in a running state on windows operating systems and shows the utility of RAM in Computer Forensics that is often neglected while crime scenario with running system is encountered. Keeping in view this necessity, it is essential to consider the issues of digital evidence and their collection, preservation, and admissibility in the court of law.

Keywords
Read Only Memory (ROM), Acquisition, Seizing, Verifying, imaging, Random Access Memory (RAM), Integrity, Authenticity, Address Resolution Protocol (ARP), Man-In-The-Middle Attack.

1. INTRODUCTION
Digital evidence or electronic evidence is "any probative information stored or transmitted in digital form that a party to a court case may use at trial". The main characteristics of digital evidence are: it is latent as fingerprints and DNA, can transcend national borders with ease and speed, highly fragile and can be easily altered, damaged, or destroyed and also time sensitive [8]. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. When dealing with digital evidence, the principles that should be applied are: actions taken to secure and collect digital evidence should not change that evidence; persons conducting the examination of digital evidence should be trained for this purpose and activity relating to the seizure, examination, storage, or transfer of digital evidence should be fully documented, preserved, and available for review.

2. CYBER FORENSICS
It is the science of extraction of evidences from digital devices without altering the authenticity of the original evidence object.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence (Judd Robbins).

3. CYBER FORENSICS: Classification
The branch of Cyber forensics can be classified into various sub branches. Some of them are:

Disk forensics deals with extracting data/information from storage media by searching active, deleted files and also from unallocated, slack spaces.

Network forensics deals with monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze wireless network traffic data.

Database Forensics relates to the forensic study of databases and their related metadata.

A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.

Malware Forensics deals with Investigating and Analyzing Malicious Code for identification of Malware like viruses, Trojans, worms, key-loggers etc. and to study their payload.

Mobile device forensics deals with examining and analyzing mobile devices like mobile phones, pagers to retrieve addresses book, call logs (Missed, Dialed, Received), Paired Device History, Incoming/Out Going SMS/MMS, Videos, Photos, Audio etc.

GPS forensics, also known as Sat-Nav. Forensics, is a relatively new discipline within the fast paced world of Mobile Device Forensics. It is used for examining and analyzing GPS devices to retrieve Track Logs, Track points, Waypoints, Routes, Stored Location; Home, Office, etc.

E-mail Forensics: Deals with recovery and analysis of e-mails including deleted e-mails, calendars and contacts.

Memory Forensics deals with collecting data from system memory (e.g., system registers, cache, RAM) in raw form and carving the data from the raw dump [7].

Table 1. Active research areas in Digital Forensics

Active Areas	Components	Related Tools
Disk Forensics	Hard Disk, CD/DVD, Flash drives	FTKs, Recovery kits
Network Forensics	Ethernet, TCP/IP, Internet	Wireshark , TCPdump
Mobile Device Forensics	Smart-phones, PDAs	Forensic desoldering
Wireless Forensics	Wireless network traffic, VOIP	W-IPS , W-IDS
Live Forensics	When encryption is in use	Pre-deployed agents
Memory Forensics	Analysis for RAM dump	WinDBG
Multimedia Forensics	Audio, Video, Pictures	Binders , Cryptors

4. CYBER FORENSICS: NEED

According the Judd Robbins, the expectations from Cyber Forensics are that it:

- **Protects the subject computer system** during the forensic examination from any possible Alteration, damage, data corruption, or virus introduction.
- **Discovers all files** on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
- **Recovers** all (or as much as possible) of discovered **deleted files.**
- **Reveals** (to the extent possible) **the contents of hidden files as well as temporary or swap files** used by both the application programs and the operating system.
- **Accesses** (if legally appropriate) the contents of **protected or encrypted files.**
- **Analyzes all possibly** relevant **data** found in special (typically inaccessible) areas of a disk.
- **Prints out an overall analysis** of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.

Cyber forensics process encompasses five key elements:

The identification and acquiring of digital evidence: knowing what evidence is present where it is stored and how it is stored is vital in determining which processes are to be employed to facilitate its recovery.

- **The preservation of digital evidence** is a critical element in the forensic process. Any examination of the electronically stored data can be carried out in the least intrusive manner. Alteration to data that is of evidentiary value must be accounted for and justified.
- **The analysis of digital evidence** relates to the extraction, processing and interpretation of digital data and is generally regarded as the main element of cyber forensics. Extraction produces a binary junk, which should be processed, to make it human readable.
- **Report the findings** means giving the findings, in a simple lucid manner, so that any person can understand. The report should be in simple terms, giving the description of the items, process adopted for analysis & chain of custody, the hard & soft copies of the findings, glossary of terms etc. [5].
- **The presentation of digital evidence** involves deposing evidence in the court of law regarding the findings and the credibility of the processes employed during analysis.

5. CYBER FORENSIC: ANALYSIS (INPUT / OUTPUT)

- **Data Recovery:** includes recovering and analyzing non-overwritten deleted files, as well as carving out portions of files and text from unallocated and slack space.
- **String and Keyword Searching:** involves looking at known and unknown files, as well as unallocated and slack space, to identify readable text within a binary file or to find a file that contains a specific string.
- **Volatile Evidence Analysis:** gives the analyst the ability to see what state the System is currently in by peering into connections, processes and cache tables.
- **Timeline Analysis:** a timeline of events is created and analyzed based on the modified, accessed and changed times associated with all files that were imaged.
- **System File Analysis**: reveals unauthorized changes to system binaries.

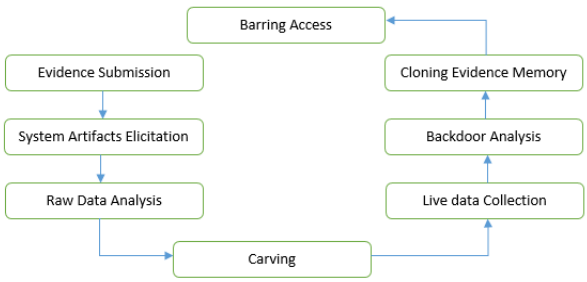

Fig 1: Brief Timeline for Digital Memory Forensic

6. FORENSIC ANALYSIS: Significance for Law Enforcement

Traditional methods of analysis in computer forensics generally involve the acquisition, seizing, verifying and imaging of hard disk or other storage media that is particularly ROM and then extracting the data for analysis [1]. But this is done after pulling the plug of the computer or shutting it down. Actually if a crime scene with running computer is

encountered, then the practice of switching it off or pulling the plug may result in loss of tones of evidence and the live acquisition becomes important. Actually in INDIA, the IOs are mostly the police officers from a non-scientific background or without the knowledge of computer science, being unable to understand the importance of RAM, rather try to shut down the system and power it off to collect the hard drive. The volatile evidence that resides in RAM can provide vital leads to investigation.

Computer Forensics is the application of science of computer, its peripheral devices and its networking for the scientific examination and analysis of data present on or retrieved from computer that might be part of illegal activity or its storage media in such a way that the data can be used as evidence in criminal proceedings that may result in punishment as decided by law [12]. This area of forensic science can involve any computer crime like data diddling, identity theft, money laundering, phishing, hacking, hijacking, child pornography, sexual harassment, uploading and downloading obscene literature/videos, infringement of copyrights, drug trafficking, human trafficking, terrorism, software theft, launching DoS attacks, email-bombing, man in the middle attack, address resolution protocol poisoning etc even beyond the boundaries of a country. The data that acts as evidence are of two types:

Persistent data: Data that is stored on a local hard drive or another medium like floppy or other attached devices like pen drives, memory cards etc. and it remains there even when the computer is turned off and disconnected from power supply. Persistent data is collected, when it is clear that evidence related to the computer crime incidents resides in the persistent storage areas only.

Volatile data: Volatile Data is the data that is irretrievable with the loss of power and it is continuously changing with time. Volatile data generally resides in RAM which would be lost if computer is turned off or restarted. The volatile data that can be recovered is date and time, running processes, network connections, network status, logged on users, doc files, email ids and login credentials, chatting messages, email messages, login credentials for social networking site, other accounts with login credentials, encryption keys, etc.

6.1 Random Access Memory: Analysis

RAM is short form of Random Access memory is found in devices like computers, printers, etc. RAM is meant to provide the memory space that can be accessed quickly. The hard drive sends data to the RAM necessary for running a given application and the processor accesses the data saved to the RAM to run the application. In this way the RAM acts as an interface between the hard drive and the processor.

However, the data in RAM stays there only as long as your computer is running or as long as the power is being supplied. When the computer is turned off, RAM loses its data. When computer is turned on again, the operating system and other programs and processes, automatically gets loaded into RAM, from the hard disk but the processes which were being used by the user before the system was turned off will not be loaded again like internet browsing, networking processes, applications being used previously etc.

RAM is memory in which all areas can be written to or read from within the same amount of time. The operating system, application programs and data in current use are kept in RAM for quicker access by the computer's processor. For example, a word processor and a spreadsheet along with the Google websites and other processes can be opened simultaneously in the RAM memory. This is how the various processes gets loaded into RAM and comes into the image to serve as evidence when imaging is done with various available tools like FTK, WinHex, Triage etc.

6.2 Virtual Memory:

But when the computer RAM gets packed to its capacity and it is not in a position to load more processes, the operating system should show the message like no more memory or no more space but it does not happen because of a pre-installed feature called virtual memory. In 1970, IBM introduced System/370, the first of its architectures to use virtual memory. Virtual memory allows many processes to share RAM simultaneously without corrupting one another's data i.e. multiprogramming and multitasking. In computing, virtual memory is a memory management technique that is implemented using both hardware and software [4]. Because the RAM has less storage space therefore every operating system use some sort of memory management technique to prevent any sort of intermingling of data of ongoing processes which are operating simultaneously [3]. This technique tackles the undesired situation by giving each process a very large address space or virtual address space for each process and divides it into pieces of memory that are uniformly sized called as pages. This memory management technique is used to map memory addresses used by processes or programs, called virtual addresses or virtual address space, into physical addresses loaded in computer's physical memory i.e. RAM [6].

SWAP SPACE: In windows operating system when RAM is packed to its capacity the processor contacts the hard disk to dump those processes that are not being used at that time, in the swap space on the hard disk or a file called as pagefile.sys and loads those files or processes that are required for immediate processing on to it but was not able to load them because of shortage of RAM space [6]. The area on disk used for this purpose is called the swap space. It can contain browsed websites, social networking site data like of facebook, searched friend list and also sometimes website account login credentials, etc.

SLACK SPACE: Slack space is defined as the space between the end of the actual file and to the end of the pre-defined area that was actually allocated to the whole of the file for storing data. A cluster is the smallest logical amount of hard disk space that can be allocated to a file for storage of data in the operating system. Now when the file does not occupy the whole of cluster that has been allocated to it, the remaining part or space of the cluster that remains unoccupied is called slack space. BUT the RAM slack is that portion of the whole slack that starts from the end of the logical file and goes up to the end of the sector but not up to the end of the cluster. This area may contain data from the previously existing files which were deleted by the user and have become history, but was not overwritten because the file length was shorter than the allocated space. Therefore the contents of the data that was processed on the computer in previous sessions, for example, traces of doc files, the websites browsed, downloaded applications or programs, or the documents browsed etc. comes into the slack when RAM is imaged [9]. This can provide leads to the investigation and sometimes act as evidence in court of law.

6.3 Hibernation and its Importance in RAM Forensics

When the system enters the mode of hibernation or sleep mode certain files get created to store all the contents of RAM and the files thus created are called hiberfil.sys. Hiberfil.sys file exists in root directory of the system partition in the hidden form as C:\hiberfil.sys. Similar to swap space, hibernation files contain mammoth information that can be used as evidence in court of law. The contents of a hibernation file can be accessed by a number of disk maintenance utilities.

SIGNIFICANCE OF VOLATILE DATA*:* If data is encrypted and the criminal is not willing to share the key then the investigator cannot access that data unless it has been cracked or recovered to decrypt data. As keys and passwords are rarely stored in hard disk by such clever criminals, it is not possible to access the encrypted data. But with volatile data all the passwords, encryption or decryption keys can be recovered as they come to play in RAM when the criminal presses them from keyboard [2]. Also when the suspect accesses an unencrypted file, the content is unencrypted and gets loaded into memory. This unencrypted content may remain in memory even after the suspect has closed the file, as long as it is not overwritten by something else [15]. This volatile memory analysis may reveal fragments of files or even whole file that would otherwise be unrecoverable if the key or password used to encrypt the data could not be discovered. Another utility is that it reveals information about processes and the applications that were running in system before being powered off.

Volatile data provides information about those Viruses, Trojans and Worms that reside only in memory not in hard disk or those Viruses, Trojans and Worms that may remove the malicious activity when system is shut down. Magistr, TROJ_BAGLE, Code Red, ROBOT-ALJ, Witty, SQL Slammer are examples of worms that live in memory and not on the hard disk.

Sometimes if only a server of a company is attacked and the company refuses to stop the machine because that could cost the company more loss than the attack, in such situations the investigating officer has to work on a live system. In this case it becomes easy to find out that if some employee is involved in the malicious activity or the attack was launched through networking from some remote point.

Running processes, network connections, open files and fragments, logged in users, etc. or any other data all provide context about the runtime state of the system that can be used for corroboration with evidence found during hard disk analysis [14]. Moreover if the system is still in a state of compromise the attacker can be reached from the established connections, opened and attacked ports, address resolution protocols, routing tables, etc.

6.4 Recovering and Analyzing Data from Volatile Memory: Tools & Techniques

The volatile data can be recovered by using open source tools and also by using licensed version tools. For this process the RAM has to be imaged to prepare a dump [11]. Then this dump has to be analyzed for recovery of evidence. There are some tools that have capability of imaging but cannot be used for analysis purpose like Triage while some of the tools can be used for capturing the RAM i.e. imaging as well as for analysis of captured memory like FTK (FORENSICS TOOLKIT from AccessData Corp.) imager, WinHEX, Encase etc.

First of all, dump file for the physical memory of windows and it's .dmp or .mem that is made by tools like task manger that is already installed in windows higher versions like win 7 or 8 or tools like FTK IMAGER, Win HEX, Encase and Triage: Incident Response, etc [10]. Some tools are used for imaging like Triage: Incident Response but some are used for analysis only like WinHex and some tools are meant for both like FTK AccessData [13].

6.5 Forensic Duplication: A Technical Introduction

Forensic duplication refers to bit stream imaging of data from the digital media in question. Data resides in all sorts of storage media present in computers, smart phones, GPS devices, USB drives, and so on. We need to be able to get to this information in a manner that it does not change the information on the devices themselves. If the evidence is not collected properly, an issue emerges where the results of the forensic exam will be put in doubt. Hence it is necessary to copy the data carefully in a forensically sound manner.

Files can be copied from suspected storage media using two different techniques:

Logical Backup

A logical backup copies the directories and files of a logical volume. It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.

Bit Stream Imaging

Also known as disk imaging/ cloning/ bit stream imaging generates a bit-for-bit copy of the original media, including free space and slack space. Bit stream images require more storage space and take longer to perform than logical backups.

When a bit stream image is executed, either a disk-to-disk or a disk-to-file copy can be performed. A disk-to-disk copy, copies the contents of the media directly to another media. A disk-to-file copy copies the contents of the media to a single logical data file.

During backups and imaging, the integrity of the original media should be maintained. To ensure that the backup or imaging process does not alter data on the original media, investigator should use a write-blocker while backing up or imaging the media.

- A write-blocker is a hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.
- When using a hardware write-blocker, the suspected storage media used to read the media should be connected directly to the write-blocker, and the write-blocker should be connected to the computer or device used to perform the backup or imaging.
- When using a software write-blocker, the software should be loaded onto a computer before the media or device used to read the media is connected to the computer

After a backup or imaging is performed, it is important to verify that the copied data is an exact duplicate of the original data.

Computing the message digest of the copied data can be used to verify and ensure data integrity. A message di-gest is a hash that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated.

Forensic image files, (i.e., Cyber Check Suite ".p01", Encase ".e01", or SafeBack ".001/.SFB" files) are written as logical files and shall be created on brand new freshly formatted media or forensically wiped sterile media if new media is not available. HDDs are to be used only once for original evidence storage.

Logical file copies of the forensic image files shall be made on brand new (sterile) HDDs before traveling back to the office. These drive copies shall be labeled as copy of hard drive, etc. Using barcode is one of the best methods. In case of non-availability of barcode, a serial code with relevant information like unit name, year, case number, etc., can be used.

Table 2. Rules of Evidence

Admissible	Can be taken account in Court of Law or elsewhere
Authentic	Relates to incident in relevant way
Complete	Exculpatory evidence
Reliable	No question about Authenticity
Believable	Clear, easy to understand, genuine

7. CONCLUSION and FUTURE WORK

This can be concluded that whenever a crime scene with running system is approached, it becomes a primary and necessary step to collect the RAM before shutting it down and removing its power supply and jumping to collect the hard disk. Otherwise, forensic scientists loose valuable information contained in RAM that may help an investigator to reach the criminal or it may be helpful in justice impartment system. The evidence like encryption keys, unsaved Microsoft documents, commands given on CMD, cryptographic documents and pictures, passwords that have not been saved on hard disk, email ids and the passwords that criminal is not willing to share, executed applications, incognito mode history of web, chatting messages, key loggers that run in the background of a computer in a stealth mode, various other ongoing processes that may be hidden or non-hidden are extremely fragile because they can be easily destroyed or overwritten by disconnecting the electric power supply to the machine or executing commands on the system and hence should be handled properly and their collection becomes very necessary as they might be helpful in justice impartment process.

In order to show the importance of RAM forensics a number of tools were used for acquisition and analysis of data or the memory collected. All those tools have shown that RAM contains a valuable data that cannot be compromised at any cost.

In today's world of 21st century, the cybercrime has reached monumental proportions across the globe and it is only expected to rise with the growing years. So, it has become extremely important for the law enforcement agencies to improve and regularly upgrade their core areas of cyber techniques for effective cyber policing. The present study aims to highlight the necessity of using latest techniques like the importance of RAM acquisition from a running system, fighting the various kinds of viruses and helping in various kinds of investigation.

Thus, the future cope of the study could be to develop a forensic framework, integrated with the efficient volatile memory analysis and visualization tools and techniques.

8. ACKNOWLEDGMENTS

Our sincere thanks to AIG H.S. Mann, with his entire Punjab State Cyber Crime Wing along with the Computer Science and Engineering Department, Thapar University, Patiala for their continuous support in carrying out the research.

9. REFERENCES

[1] Remzi H. Arpaci-Dusseau, Andrea C. Arpaci-Dusseau, Operating Systems: Three Easy Pieces, Arpaci-Dusseau Books, (2014), 13, 5, (0.80 edition)

[2] Carsten Maartmann-Moea, S.E. Thorkildsenb, A.Arnesc, The persistence of memory: Forensic identification and extraction of cryptographic keys, J. digital investigation , (2009), vol. 6, S132–S140

[3] A. Aljaedi, D. Lindskog, P. Zavarsky, R. Ruhl, F. Almari, Comparative Analysis of Volatile Memory Forensics Live Response vs. Memory Imaging, IEEE International Conference on Privacy, Security, Risk, and Trust, and.IEEE International Conference on Social Computing, (2011)

[4] B.D. Carrier and J. Grand, A hardware-based memory acquisition procedure for digital investigations, J. Digital Investigation, (2004), vol. 1, 50-60

[5] https://www.sciencedirect.com/science/article/pii/S0167404804000100

[6] P. J. Denning, Virtual memory, J. ACM Computing Surveys, 2, (1970), Vol. 2 (3), 153-189

[7] https://forensicswiki.org/wiki/Memory_analysis

[8] Andrew S. Tanenbaum. Modern Operating Systems. Prentice Hall, Inc., Upper Saddle River, New Jersey 07458, (2001), 3, 194-198, 4th Edition

[9] https://resources.infosecinstitute.com/memory-forensics/

[10] F. Gianni, F. Solinas, Live Digital Forensics: Windows XP vs Windows 7, IEEE International Conference on informatics and applications (2013)

[11] S. Thomas, K. K. Sherly, S. Dija, Extraction of memory forensic artifacts from windows 7 RAM image, IEEE International Conference on Information and Communication Technologies (2013)

[12] Sid Leach Snell & Wilmer LLP, What Every Lawyer Needs to Know About Computer Forensic Evidence in IP Litigation, University of Texas 11th Annual Intellectual Property Law Symposium, February 19, 2010

[13] Steve Bunting, EnCase Computer Forensics. The Official EnCE: EnCase Certified Examiner Study Guide, John Wiley & Sons, 2012, page no.65, 3rd edition

[14] L. Wang, R. Zhang, S. Zhang, A Model of Computer Live Forensics Based on Physical Memory Analysis, IEEE 1st International Conference on Information Science and Engineering (2009)

[15] Gerard O'Regan, A Brief History of Computing (2012) ,2nd edition, 2, 27-30