ISSN:2229-6093

IJCTA

Dilpreet Singh Bajwa et al, International Journal of Computer Technology & Applications,Vol 7(3),357-367

A Comprehensive Review of Volatile Data Forensics

Dilpreet Singh Bajwa
Research Scholar, DCA
Panjab University, Chandigarh
pu.dilpreetbajwa@gmail.com

Dr. Satish Kumar
Associate Professor, DCA
Panjab University, Regional Centre, Hoshiarpur
satishnotra@yahoo.co.in

ABSTRACT

Volatile data forensics is a new challenging field required attention. Volatile data forensics must consider be a part of digital forensic process rather than individual process. It provides important and crucial information not acquired by following traditional forensic process. While we are following traditional forensic process, the important information like current state of system, running processes, open ports, recent established connections, username and passwords, unencrypted data and keys, traces of malwares and anti-forensic activities may be missed out which are present in volatile memory of system while system is in running state.. Volatile data is a source of this type of information and leads investigation fast in right direction. This paper provides a detailed view of need, challenges, tools, techniques required for volatile data forensics and importance of this field in digital investigation process.

Keywords: Digital Forensics, Computer Forensics, Memory Forensics, Volatile Data Forensics, Cyber Forensics Tools.

1. INTRODUCTION

Various types of cyber crimes and computer attacks are on rise. With advancement in technology and growing use of internet also made impact on rise of these crimes. To counter these malicious activities and to punish culprits in court of law, Digital forensics came in to existence. It is used to track and prosecute criminals involved in unauthorized activities. Although digital forensics has broader base than computer forensics as it covers all digital devices but in this paper the term digital and computer forensics used as synonym. Conventional forensics focuses on the acquisition and analysis of non-volatile data that is stored on digital storage media (e.g. hard disk). The data exists on these digital devices are permanent in nature and stored at specific location in a format defined by file system. Due to non-volatile in nature, its integrity can be verified and also post acquisition and analysis can be performed in a forensically sound manner [1]. This type of investigation generally consider as post- mortem analysis as they are performed on in-active systems. Static analysis has some limitations as it does not provide complete picture of events [2].

During traditional forensics practice the dynamic state and volatile data of the system is not preserved which is the reason for lost of precious information like running process list, open network connections, encrypted data, passwords and malicious code which only reside in RAM. Due to this reason and to save state of system, volatile data forensics is considered necessary research area for cyber forensic practitioners and investigators. Memory forensics or Volatile Da

ta forensics is in its infancy but it is growing fast and considers promising area for field of computer forensics. Memory forensics involves the capture and analysis of volatile memory such as RAM. Data is considered volatile when it is likely to be lost when a machine is rebooted or overwritten during the course of the machine's normal use [3].

This rest of the paper is organized as follows: Second part provides the reasons for need of volatile data forensics in digital investigation process. Third part discusses tool and techniques generally used for acquisition and analysis of volatile data. The detailed working of these tools is out of scope of this paper. In fourth part challenges faced and consideration any investigator keeps in mind while performing volatile data forensics are discussed. Fifth part provides conclusion.

2. NEED OF MEMORY FORENSICS

Volatile data forensics came in to lime light after DFRWS memory analysis challenge in 2005, which was focused on research and tool development for memory forensics [4, 5]. Memory forensics play very important role in forensics investigation. Volatile data forensics does not consider as an extra task but rather consider as an integral part of digital investigation process [4]. Memory forensics is extremely crucial and become increasingly important to gather necessary evidence and to make chain of events happen recently.

Following are the reasons for which memory forensics is important and also overcome limitations of traditional forensics:

Keys and Passwords: The forensic investigator cannot access data if hard disk or some files are encrypted until he recovers the key or cracks the password. Passwords and keys are rarely available on hard disk. Both encryption and decryption takes place in RAM and unencrypted data never stored on hard disk [4]. But when computer user type the password or decrypt the data, the passwords and keys are loaded in to RAM and later analysis of this volatile data can recover them.

Processes: When processes are running, space is allocated to them in memory. There are different segments like Code Segment, Data Segment, Heap Segment and Stack Segment corresponding to a process. Different types of processes are available in memory. Currently running processes as well as the processes which are terminated are also present in memory (if the space allocated to them is not overwritten and system is not rebooted). The state of these processes can be recovered by analyzing memory. The information getting from running processes can also provide insight in to how programs were used and what resources were accessed or manipulated when system is being attacked

Malwares: Some malicious code in form of virus, worms, Trojans and root kits may be present in memory. Attackers now follow a new strategy to run malicious code from memory instead of storing and leaving any trace on hard disk. After removing power from the system, there is no trace of such malwares. nimda [6, 7], Code Red [8,9] and SQL Slammer [8,10] are examples of such malwares. Current anti-virus software are not so capable to detect malicious code in memory so these malwares remains in memory and cannot be traced through traditional forensics approach. So Memory forensics required for handling such threats and possibilities.

Network details: Network information itself dynamic in nature and constantly changing. We can get the latest information regarding network, opening ports and recent established connections and their state by analyzing memory. This information we get after analyzing volatile memory is useful because the results produced by tools that are run on the machine itself, such as netstat, can be manipulated by a malware or malicious user to provide wrong information [3]. Information collected directly after analyzing the memory is considered more authentic, reliable in comparison to information collected from hard disk and has lesser chance of being manipulated.

Network details collected from volatile memory provide possibility to trace the origin of attack and to identify the culprit [11].

Unencrypted/Hidden Data: There is possibility that data we find in RAM cannot be available on hard disk. Some attackers intentionally hide data, tools, malwares and other confidential information in memory because it is difficult for investigator to detect and analyze this hidden information from conventional forensic process. Volatile memory also contain unencrypted data because when the user access encrypted data by using password/key that data in unencrypted form is loaded in to memory. This data is available in memory if files are even closed by the user and later if it is not overwritten can be acquired and analyzed by accessing volatile memory.

Anti-forensics: According to [12], anti-forensics consider as one of the future challenge for Digital forensics process. According to Harris, by anti-forensics we mean any attempt to counter availability of useful data/evidence to the forensic investigation [13]. One of the techniques in anti-forensics is use of Memory resident compiler/assemblers: This technique allows tools to be compiled for the compromised platform, but, more importantly, to be compiled on the fly in memory (inside a hijacked process) so as not to leave a trace on the local disk [14]. Volatile data forensic also helps in finding traces of such anti-forensic techniques.

Internet information/message chats: Web version of instant messaging service like Windows Live Messenger, Google Talk, etc. change the scenario today as they posed as a new challenge for forensic investigators because they does not leave any trace on hard-disk but while the user using them, they dump some part or complete record in memory. When we close the web browser or shutdown the computer, this data is lost. So to access or collect this type of data which prove to be very useful information, volatile data forensics can be used [15, 16].

3. TOOLS AND TECHNIQUES

The most important part in volatile data forensics is to first acquire the memory and after that analyze it to produce evidence. Many tools commercial, free as well as open source are available for acquisition of memory and analysis afterwards. No tool is perfect and poses challenges especially in case of acquisition because memory is volatile and acquisition must be done on live system. The analysis and results/evidence produced depends upon the successful acquisition of memory. Fundamentally, memory acquisition is the process of copying contents of memory to another persistent storage media for later analysis. Another appropriate description about imaging in case of volatile memory is sampling of the state of physical memory at given point in time. The state of the physical memory as a whole cannot be directly measured but can be deduced from state of these individual samples [17]. Several issues need to consider while acquiring volatile memory, we discuss main issues investigator faced during acquisition of memory in the next section. The methods and tool used particularly during investigation process depends upon the characteristics of investigating system and goal of investigation process [17]. But the main requirement is that they must provide reliability and consistency during acquisition and produce authentic and valid results during analysis. In this section first we discuss popular methods and tools for acquisition of memory and later on about methods and tools used for analysis.

3.1 Acquisition Phase for Volatile Memory

The memory acquisition can be performed in different ways, each have their own benefits and drawbacks. Broadly categorize in to Hardware versus Software based acquisition.

3.1.1 Hardware Based Acquisition

Hardware base acquisition has the ability to create more atomic image of memory [16]. Hardware acquisition techniques are quite limited and can be possible by use of dedicated hardware only.

Hardware-based acquisition use direct memory access (DMA) without involving computer's processor. It has biggest benefit that it cannot alter the contents of Memory during acquisition as it is not the case with software based acquisition. Even if the system is corrupted or compromised, still we get the valid image of memory. First specialized hardware designed specifically for this purpose is the Tribble Card [3, 16, 18] which is a PCI card based solution and must installed on the system prior to some compromise takes place. Further some vendors like Intel and AMD provide technologies (VT-d, IOMMU) to restrict PCI based cards to access memory due to security precautions[8]. Another solution is Firewire controller [16, 19] but Firewire can only support first 4GB of RAM [17] Other solutions include Thunderbolt and Expresscard [17]. The disadvantage associated with hardware based acquisition is that you need dedicated hardware which is expensive and must install these cards before some compromise takes place on your system.

3.1.2 Software Based Acquisition

An option is also provide by some operating system to provide an interface, (In Windows \\.\Device\PhysicalMemory, \\.\DebugMemory, in Linux /dev/mem, /proc/kcore) to inspect memory [3, 16] but modern operating systems either restrict or remove this feature because of security concerns.

Due to restrictions imposed on memory interfaces, software companies built dedicated tools for memory acquisition. No tool is perfect, so as a forensic investigator you need collection of tools that fit according to investigation process and system configuration. While choosing software acquisition tools must take care that the footprint of any tool must be minimal otherwise they can overwritten potential evidence. The acquired image of memory can be stored on removable media or saved across network not on hard disk of system otherwise can harm important evidence.

Some of the tools are discussed here use for memory acquisition: Tools such as dd can be used from a live CD to copy contents of memory. Similarly win32dd [16, 20] and mdd [16, 21] used for memory acquisition. Helix3(dd) [22, 23] is a tool can use for memory acquisition and has a graphical user interface. Nigilant32 [22, 24] is developed by agile Risk Management and is an open source tool. It takes live system snapshot and acquire network information, process listing, user information and processes etc [22]. GMG Systems, Inc., KnTTool contains remote deployment module, evidence collection over SSL, cryptographic integrity checks, automatic collection of live user state data, it can also capture ROM, NVRAM, EEPROM, from the BIOS and Peripheral device memory. MoonSols Windows Memory Tool Kit (MWMT) contains win32dd, win64dd and also contain most recent version of utility DumpIt used for 32 and 64 bit memory acquisition tools with just a single click. AccessData FTK Imager supports capturing of various type of data in RAM including chat logs and network information, Most popular commercial software Encase/WinEn from Guidance software can also record metadata in headers and acquire memory in compressed format. Belkasoft Live RAM Capturer also having capability to acquire memory even in presence of anti dumping mechanism. It can also rum from a USB drive and support both 32 and 64 bit major versions of windows. HBGary Fast Dump can acquire physical memory in to a single HPAK output file and also claims to leave smallest possible footprint during acquisition. Mandiant Memoryze supports capturing of memory from removable device and its output can be imported in to Mandiant Redline for graphical analysis. Fresponse also tool used for memory acquisition from remote location. Winpmem is an open source memory acquisition tool used for windows. It also has capability to support different output format like raw or crash dump. ATC-NY Windows Memory Reader can also send output to a remote netcat listener. Each tool have their own limitation, some support 32 bit, some 64 bit configuration and some only support acquisition of up to 4 GB, some vary in their output formats

and so on. In [22], author compare FTK Imager, Pro Discover, Win32dd, Nigilant32, Memoryze and Helix3(dd) volatile data acquisition tools and conclude through their experiment that GUI tools are comparatively easy to learn than command line tools, the time require to acquire memory image is proportional to its size and Win32dd and memorize is suitable option acc. to time constraint. All the tools leave footprints which will negatively affect the investigation.

Other acquisition Techniques is to take full crash dump of memory. It can occur under some certain condition having no control of user or can be force the crash by using built in CrashOnCtrlScroll [6, 26] or by using utility NotMyFault.exe of SysInternals, now part of Microsoft [6]. This method however copies the complete memory on disk but there are chances to overwrite potential evidence available on disk.

Another method used for memory acquisition depends upon persistence of memory data during warm booting. It is known fact that volatile data persists when rebooting the system [16, 27] It depends upon the hardware design, type of memory and also on version of operating system. While rebooting the system some tools take a dump of memory and stored it in removable media. It is like crash dump method but the dump is stored on external USB media not on system's hard-disk. Afterlife is an example of such tool that used this method. It produces very few footprints on memory approx 1 MB. It has 4 GB acquisition limit [16, 27].

3.1.3 Another method

To acquire memory is dependent on persistence power of memory after power is off. DRAM's used in modern computers have this capability to retain their contents for few seconds when power is off, even when removed from motherboard and at room temperature. The dta can retain for minutes and hours if memory can be kept at low temperatures. The decay of bits takes place with time can be prevented by keeping chips at extremely low temperatures for example we can maintain surface temperature of approx -50° C by using canned air duster spray on chips, the decay in this case is 1% after 10 minutes. If we use liquid nitrogen to submerged chips, it can maintain temperature of approx -196° C and decay in this case is 0.17% after 60 minutes without power. Different methods can be proposed by [28] to acquire memory. One method is to remove RAM an transferred it by using "canned air" dusters or compressed fluorohydrocarbon refrigerant to another machine and extract their state by using customized kernels.

Above we discuss the techniques and tools we generally used for memory acquisition. Now we are discussing analysis tools and techniques that is how to extract information/evidence from our memory dump.

3.2 Analysis Phase for Volatile Memory

The analysis very much depends upon the reliability and authenticity of memory acquisition because if our memory dump is corrupted or not reliably taken then the evidence and information we collect during analysis is not consider authentic.
Before discussing available tools and techniques for analysis of memory, we discuss resulting formats produced after acquisition of memory for analysis.

3.2.1 Memory Dump Formats:

When we acquire memory then the resulting dump is saved in various file formats depends upon the tool, technique or format we chosen.

3.2.1 Memory Dump Formats Available for Analysis

Various types of formats are existing like Raw memory Dump is most widely used format, it does not carry any meta data and header information for their identification, Windows Crash Dump, designed for debugging process, they itself comes in various types like kernel dump, small or memory dump and complete memory dump [17,

29]. Hibernation file format (hiberfile.sys) is compressed copy of memory produced during hibernation procedure. During hibernation, the system active connections can be terminated and also malwares can remove their trace from memory, so investigator does not be able to get this information from hibernation file [30]. First MoonSols developed Sandman Tool, Another format widely used id Expert Witness Format (EWF) produced by mainly EnCase tool, Another format HPAK designed by HBGary, it is proprietary format and the sole tool produced this format is FastDump. Other formats also available which involves virtual machine: While using product like VMWare, we can take a snapshot by just pausing or suspending the Virtual Machine and saves the copy of memory dump in host's the file system. VMware's either contained memory in to a single .vmem file or can also save state and metadata in .vmsn and .vmss files in addition to .vmem fle . Mainly while we analyzing these dumps through some analysis software like Volatility, we required all three files to get better picture as .vmem stores physical memory and other files contain metadata which is helpful to get accurate information about the memory. While using VirtualBox, automatic dump is not created on suspend and pause. We can either use VirtualBox Python API (vboxapi) to create our own utility for memory dumping or either can use vboxmanage debugvm command [17, 31] to produce ELF64 core dump or can use .pgmphystofile command [17]. QEMU is just like VirtualBox, investigator can create dumps by using virsh [32]. Actaeon is another tool for acquisition of memory of virtualization environments. Starting from a physical memory dump, Actaeon perform three main functions: one, locate the Hypervisor (virtual machine monitor) that uses the Intel VT-x technology, second, nested virtualization can be detected and analyzed and also show relationship between separate hypervisors running on same host [33].

We can also convert one format in to another, tools are available for this. Generally the analysis tools support one or two formats except Volatility Frame work which supports many formats. So there is need to convert the acquired memory dump in particular format in to another format understand by investigator's analysis tool. MWMT converts hibernation file and crash dumps in to raw format. VMware's vmss2core.exe file can convert .vmsn (snapshot or saved state) in to crash dumps. Vm2dmp of Microsoft can create crash dumps from microsoft Hyper-V files. Volatilty imagecopy plugin create raw memory dump from crash dump, VMWare, QEMU, EWF, FireWire, hibernation file, VirtualBox file formats and raw2dmp plugin can convert raw memory dump in to crash dump [17].

3.2.2 Tools and Techniques used for Memory Analysis

After acquiring the image of volatile memory, the investigator want to analyze it and earlier the most popular method is string search to find anything recognizable. In Unix string utility is used for this and it also been ported to windows as well. In windows other GUI tools are also available for string searching. XORSearch [34] is a tool used for specific searching based on keywords provided by analyst. XORStrings is best described as the combination of XORSearch tool and the well-known strings command. XORStrings will search for strings in the (binary) file you provide it, using the same encodings as XORSearch (XOR, ROL, ROT and SHIFT).

Some tools which are inbuilt or can installed on system are netstat, ps, isof, ipconfig, Sysinternals, resourcekits, although they are not good from forensic point of view because on executing they can change state of system and secondly as they are executed on system itself, their results can be manipulated by malwares present on compromised system. But as they provide useful information from volatile memory that is why discussed here: like Netstat is the tool used for getting network information including listening ports and active connections, lsof shows the corrently open files on maschine and ps shows currently running processes on system. Ipconfig shows network interface configuration details. Other tools that are not part of System but can be installed to get

specific details about processes, open files etc. are resorcekits for windows, Foundstone tools and Sysinternals maintained by microsoft.
Generally the analyst brings their own set of tools on some USB drive or CD needed for forensic investigation. KnTTool is used for acquisition and analysis, the analysis module is called KnTList and used for reconstructing the data structures of Windows and produced output in XML Format. FATKIT [35] is a toolkit developed by Petroni et.all and allows analyst to reconstruct virtual address space and visualization and kernel analysis for Windows and Linux. It allowed analyst to write scripts for extraction of evidence according to their custom requirement and also has the capability to detect malicious code. WMFT is another analysis tool for volatile data from Windows 2000, 2003 and XP. Before using WMFT, the analyst first locate symbols point to important structures and objects in memory and after that plug the values corresponding to pointing memory locations and analyze the data structures to extract important objects and processes from memory [36]. It is vulnerable to attacks where attackers change data structures like linked lists used by kernel to point objects and processes in memory [3]. Idetect is also analysis tool used only for linux that extract detailed information from memory image about active processes and also information about structure related to process.

Volatility Framework [17, 37] Volatility Framework is an open source collection of tools used for analysis of memory samples and it is wide popular among forensic community. It is implemented in python and provide a single cohesive framework for memory analysis of 32, 64 bit Windows, Mac and Linux Systems. It supports number of commands for various uses like to open list of DLL files, open active connections, print memory map corresponding to memory dump in question, also used in malware analysis and produce executable from its associated process.

VAD Tools [3, 38] VAD tools are collection of python scripts use to extract information about processes, process structures from Virtual Address Descriptor Structures of memory and have ability to reconstruct .dll or .exe file. Five scripts vadwalk.py, vadinfo.py, vaddump.py, procdump.py and listdll.py are used for this purpose. Encase [3, 39] from Guidance Software is most widely used commercial forensic utility. It allows capture of volatile data from RAM. It does not provide raw dump of data rather only provide interpretation of data. F-Response another tool provide remote read only acess to memory and for acquiring memory some another tool is required in collaboration. HBGary is a powerful tool used for analysis and provides malware analysis capability. It allows extracting, disassembling and scanning malicious code and its functionality. It also contains FastDump utility to capture memory.

4. CHALLENGES IN VOLATILE DATA FORENSICS

Volatile Data acquisition and analysis is not so daunted task if we consider them separate from forensic process because tools and techniques are available or under development and research is going on how to acquire and analyze the volatile memory. Further by using these tools and techniques if not complete, we extract lots of useful information and also identify crimes and culprits but real challenge comes when we talk about Volatile Data Forensics. The same tasks acquisition and analysis now considered more difficult because now we don’t only acquire or extract memory information but has to extract evidence in a manner which is reliable, authentic, valid, tested and admissible in court. We must have to prove our process, tools, techniques, collected evidences in court of law under legal norms. So there must be some framework like traditional forensic process to acquire and analyze volatile memory and also maintain chain of evidences under standard procedure. Need to develop tools and procedures which are not only efficient but forensically sound also. So Volatile Data Forensics is in its infancy and in itself is a challenge. Tools procedures and techniques are developing with time. Several issues arise while the investigator performs the task of memory

forensics and there is need to address those issues in ongoing research and development of Volatile Data Forensics.

Tools effect on Memory: One major concern regarding volatile data forensics is that while acquiring memory by using software acquisition technique can cause changes to the system. When we used some tool to capture volatile RAM, it is loaded and produces changes in RAM or overwrites some data which may be some potential important information. This happens due to use of some portion of memory by tool to conduct its task. So it must be take care of that the acquisition tools used can leave smallest footprints on memory and investigator also differentiate between the information present in memory and what changes takes place after use of tool so that he properly analyze the memory. Generally GUI tools leave more footprints than command line tools. Hardware acquisition techniques are used to avoid this problem but they have their own drawbacks.

Integrity check problem: In traditional forensics we make an image of non volatile device like hard-disk on an inactive system and later on analyze it to produce evidences but before that we also check integrity of the system by applying md5, sha1 etc algorithms to calculate hash values for both original and copied data and prove that original and duplicate copy are containing same data. This thing is not possible in case of volatile data because the state of the system is not consistent. When we start copying process and when we end it, at both times system state is different. So it is impossible to check or verifying integrity of volatile data [1, 40].

State Preservation: During acquisition of memory, the system is in live state and the state of system is constantly changing. You cannot create memory of image at particular point in time. During acquisition, it is impossible to freeze system state while it is running. Even the best methods introduced some difference of time between the acquisition of first and last bit. So if the acquired system is inconsistent, it is difficult to prove authentication of results produced in court [1].

Lack of Structure: The data stored in RAM is structureless compare to data store on hard-disk where file system is there to store and retrieve data and have predefined format. Investigation relies on concepts like file allocation table, inodes, master file table etc. which is not the case with RAM. Generally for analysis techniques like kernel debugging and reverse engineering can be used. Processes structure is defined while they are residing in memory but less information is available due to security concerns in case of proprietary operating systems and it differs between different versions [6].

Malwares/Anti-forensics: Malwares are the malicious codes having some bad intent. Traditional forensics focus on analysis of only persistent data available on hard-disk so attackers find new way to hide their malicious code and data in memory. They leave no trace on hard-disk and also had capability to manipulate forensic results. Anti-forensics are the techniques to hinder forensics process. Harris, defined anti-forensics as comprises any attempts “to compromise the availability or usefulness of evidence to the forensics process” [41, 42] Apart from traditional anti-forensic techniques the new techniques allow to use software to be present in RAM only and also Granfinkel [41, 43] speculate that these anti-forensic tools can directly attack forensic tools by finding vulnerabilities in it.

5. CONCLUSION

Volatile data forensics is important because it helps to acquire and extract information that is not possible with traditional forensic practices. Further it supports conventional data forensic process and can be considered as an extended part of it. Volatile data forensics is a new area and requires more consideration and research. This paper is an attempt to provide a comprehensive overview of volatile data forensics, its requirement in forensic field and challenges face by investigators. Paper also discusses the tools and techniques require for

acquisition and analysis of volatile data. More specifically paper discuss about RAM, not much consideration given on volatile data associated with other digital devices like mobile phone, network devices etc. but the core concept remains the same for other devices also.

REFERENCES

1. Y. W Frank Law, K. P Chow, Y. K Michael Kwan, K. Y Pierre Lai, "Consistency Issue on Live System Forensics", "Future Generation Communication and Networking (FGCN)), Vol-2, pp 136-140, IEEE, 2007.
2. Sasa Mrdovic, Alvin Huseinovic, Ernedin Zajko, "Combining Static and Live Digital Forensics in Virtual Environment", International Symposium on Information Communication and Automation Technologies (ICAT) XXII, pp 1-6, IEEE, Oct-2009.
3. Kristine Amari, Carlos Cid, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory", SANS, March 2009. Available at: https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049.
4. Aaron Walters, Nick L. Petroni, Jr., "Volatools: Integrating Volatile Memory Forensics into Digital Investigation Process", Available at: https://www.blackhat.com/presentations/bh-dc-07/Walters/Paper/bh-dc-07-Walters-WP.pdf.
5. DFRWS, "DFRWS Forensic Challenge". http://www.dfrws.org/2005/challenge/
6. Timothy Vidas, "The Acquisition and Analysis of Random Acess Memory", "Journal of Digital Forensic Practice", 1:4, pp 315-323, Jun-2007.
7. "CERT Advisory CA-2001-26 Nimda Worm", Revised: 25 September 2001. Available at: http://www.cert.org/advisories/CA-2001-26.html .
8. Jiang Wang, FengWei Zhang, Kun Sun, Angelos Stavrou, "Firmware-assisted Memory Acquisition and Analysis for Digital Forensics", Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), pp 1-5,May 2011. IEEE
9. CAIDA, "CAIDA Analysis of Code Red". Available at: https://www.caida.org/research/security/code-red/.
10. XForce, "SQL Slammer worm propagation" CVE-2002-0649, Available at: https://exchange.xforce.ibmcloud.com/vulnerabilities/11153.
11. J. Buric, D. Delija, "Challenges in Network Forensics", 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),pp 1382-1386, IEEE, 2015.
12. M. Al Fahdi, N. L Clarke, S. M Furnell, "Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions" "Information Security for South Africa" pp 1-8, IEEE, Aug 2013.
13. R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", "Digit. Investig." vol. 3, pp. 44–49, Sep. 2006.
14. Computer Forensics and Anti-Forensics Research, "Anti-Forensics Overview", Available at: http://www.forensics-research.com/index.php/anti-forensics/.
15. Ya Ting Chang, Min-Ju Chung, Chin-Feng Lee, Cheng-Ta Huang, Shiuh –Jeng Wang," "Memory Forensics for Key Evidence Investigations in Case Illustrations", Eighth Asia Joint Conference on Information Security (Asia JCIS), pp 96-101, IEEE, July 2013.
16. Timothy Vidas, "Volatile Memory Acquisition via Warm Boot Memory Survivability", 43rd Hawaii International

Conference on System Sciences (HICSS), pp 1-6, IEEE, Jan 2010.
17. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, "The Art of Memory Forensics", Detecting Malware and Threats in Windows, Linux, and Mac Memory", John Wiley & Sons, 2014.
18. Brian D. Carrier, Joe Grand, "A Hardware Based Memory Procedure for Digital Investigation", Digital Investigation, Elsevier, Vol-1, pp 50-60, Feb-2004.
19. Michael Becher, Maximillian Dornseif, Christian N. Klein, "Firewire – all your memory are belong to us", CanSecWest/core05, May 2005. Available at: https://cansecwest.com/core05/2005-firewire-cansecwest.pdf.
20. Win32dd by Matthieu Suiche.
21. mdd by Mantech.
22. Leonardo Carvajal, Cihan Varol, Lei Chen, "Tools for Collecting Volatile Data: A Survey Study", International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), pp 318-322, IEEE, May 2013.
23. Helix3, Efense, Available at: https://www.e-fense.com/store/index.php?_a=viewProd&productId=11.
24. Nigilant32, Agile Risk Management.
25. http://sourceforge.net/p/sleuthkit/mailman/message/751480/
26. KB244139, windows feature allows a memory dump file to be generated with the keyboard", last Reviewed: 9-11-2011. Available at: https://support.microsoft.com/en-us/kb/244139.
27. Jim Chow, Ben Pfaff, Tal Garfinkel, Mendel Rosenblum, "Shredding your garbage: Reducing data lifetime through secure deallocation", 14th USENIX Security Symposium, pp. 331–346, Aug. 2005.
28. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, "Lest We Remember: Cold Boot Attacks On Encryption Keys", Proc. USENIX Security Symposium, 2008.
29. CC Hameed, "Understanding Crash Dump File", Last Reviewed: Jan 2008. Available at: http://blogs.technet.com/b/askperf/archive/2008/01/08/understanding-crash-dump-files.aspx.
30. Matthieu Suiche, "Windows Hibernation File for Fun n Report", Available at: https://www.blackhat.com/presentations/bh-usa-08/Suiche/BH_US_08_Suiche_Windows_hibernation.pdf.
31. VBoxManage, https://www.virtualbox.org/manual/ch08.html#vboxmanage-debugvm.
32. http://libvirt.org.index.html
33. http://s3.eurecom.fr/tools/actaeon/
34. Didier Stevens, "XORSearch & XORStrings, http://blog.didierstevens.com/programs/xorsearch/
35. Nick L. Petroni Jr., AAron Waltersb, Timothy Frasera, William A. Arbaugh, "FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory", "Digital Investigation, Elsevier", Vol-3, pp 197-210, Dec 2006.
36. Mariusz Burdach, "An Introduction to Windows Memory Forensic, July 2005. http://forensic.seccure.net.
37. Volatility Framework, "Volatility Foundation". http://www.volatilityfoundation.org/, https://code.google.com/p/volatility/
38. Dolan-Gavitt, VADTools. Source Forge, 2007. http://vadtools.sourceforge.net/
39. Encase, "Guidance Software". http://www.guidancesoftware.com/
40. Mariusz Burdach, "Finding Digital Evidence in Physical Memory", Black Hat Federal, Jan 2006. https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Burdach/bh-fed-06-burdach-up.pdf.

41. Martin Wundram, Felix C Freiling, Christian Moch, "Anti-Forensics: The Next Step in Digital Forensics Tool Testing, Seventh International Conference on IT Security Incident Management and IT Forensics, pp 83-97, IEEE, 2013.
42. R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," Digit. Investig., vol. 3, pp. 44–49, Sep. 2006.
43. S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," "in Proc. 2nd International Conference on Information Warfare and Security", pp. 77–84. 2007.