Exploring Static and Live Digital Forensics: Methods, Practices and Tools

Mamoona Rafique, M.N.A.Khan

Abstract— Analysis and examination of data is performed in digital forensics. Nowadays computer is the major source of communication which can also be used by the investigators to gain forensically relevant information. Forensic analysis can be done in static and live modes. Traditional approach provides incomplete evidentiary data, while live analysis tools can provide the investigators a more accurate and consistent picture of the current and previously running processes. Many important system related information present in volatile memory cannot be effectively recovered by using static analysis techniques. In this paper, we present a critical review of static and live analysis approaches and we evaluate the reliability of different tools and techniques used in static and live digital forensic analysis.

Index Terms— Digital Forensics, Virtual Machine, Live Forensic, Memory Forensic, Incidence Response, Hard Disk Image. Memory Analysis

1 Introduction

As we know that the people trends about the technology have been adopted a lot of changes towards modern technologies in the last few decades. People use different digital media like PC, PDA, laptop, mobiles and some other digital devices frequently and use them for communication purposes. One major source of communication is internet, which may lead to some cyber or malware attacks, which results in damages like data theft or malicious system activities. People which have the responsibility to countercheck such cyber or malware attacks are needed to update their abilities and procedures to prevent or minimize such attacks.

Computer based crimes includes transferring or downloading digital files illegally from illegal weapons plans to child pornography to download unsanctioned music. Computer crimes includes fraud or theft related to branded computer hardware or valued software, applications or other cerebral property interests. Experts of digital forensics reconnoiter the defendant's computer files to conclude how and from which source the pirated files, unlawful, software or pirated files instigated.

Cell phones contains personal data. Digital forensic experts can access important information concerning a contacts and communications by scrutinizing digital cell phone records of that person with his telephone billing records and also other digital data collections such as ATM and credit card records.

Digital forensics relates to data files and software, computer operations, also the electronic files or digital contained on other technology based storage devices, like PDA, digital camera, mobile phones, etc. The objective of forensic science is to determine how digital evidence can be used to recreate, identify suspects to analyze or diagnose the victim machines. This analysis is used for to investigate evidences in criminal or civil courts of law. In computer forensics experts analyzes techniques and investigation to preserve evidence and gather data from computing devices. Its goal is to perform an organized investigation however, maintaining evidence to discover what happened on a computing devices and who is responsible for it. Digital forensic analysis constitutes on different processes like data acquisition, analysis and evidentiary presentation of data. It is commonly done in different modes like live and static. Static analysis is a traditional approach in which system is analyzed forensically after taking the memory dump and shutting down the system, while on the other hand in live digital forensic analysis the evidentiary data is gathered, analyzed and is presented by using different kind of forensic tools, and the victim system remains in running mode.

1.1 Static Analysis

By traditional digital forensics it is focused on examining a duplicate called copy of disk to take out memory contents, like the files which are deleted, history of web browsing, file fragments, network connections, opened files, user login history etc. to create a timeline which gives a view i.e. partial or summary statics about the activities performed on the victim system before shutting it down. In static analysis different kind of software and hardware tools like Fundl, RegCon are used for memory dumping and sorting of evidentiary data for analysis and presentation purpose. Forensic data is acquired by using different kinds of external devices like USBs, external hard derives etc. or CD,DVDs and then this data is brought into the forensic lab for investigators to perform different kinds of operations/steps to forensically analyze evidentiary data.

- *Mamoona Rafique is currently pursuing Masters Degree program in Software Engineering in Department of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan. E-mail: mamoonarafique@yahoo.com*
- *M.N.A. Khan received his PhD degree in Computer System Engineering from University of Sussex, Brighton, UK. His research interests are in the areas of Artificial Intelligence, Computer Forensics, Cloud Computing and Software Engineering. Islamabad, Pakistan. E-mail: mnak2010@gmail.com*

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

1.2 Live Analysis

New challenges are presented by the field of live forensic analysis which includes non-interactive analysis and data snapshots, which requires the progress of fresh data models and the designs of user interface.

In live digital forensics, information is gathered, analyzed and reports are generated, while the compromised system remains functional, the tools used for live digital forensic analysis can provide very clear pictures of knowledge such as memory dumps, running processes, open network connections and unencrypted versions of encrypted files, while such memory contents cannot be acquired properly in static analysis. It means that the live analysis provides the consistency and integrity of forensic data. This gathered information can be used in different ways to produce forensic evidence or to represent the forensically activities and actions performed by user directly or by remote login on that compromised system.

1.3 Live vs. Static Analysis

Static analysis is the traditional forensic investigations that are executed on such data which is at rest, for instance, the different contents of a hard drive. Investigators shut down the different computer systems due to their confiscation of dread that the digital time bombs could affect and remove the data.

In present and recent years, there is given more stress to perform study on live systems and it is increased. First reason is: Against different computer systems maximum recent attacks leaves nothing in matter of evidence and trace on the hard drive of computer. The memory of computer is only exploited by these attacks. Another factor of this cause is the more utilization of cryptographic storage, keys copy to decrypt the computer's memory storage, causes the information to be lost by turning off the system.

Different areas of live and static forensics are discussed in this paper, which includes the different kinds of information which can be collected, and the way how evidence could be studied and the way how it works in conjunction with different traditional and old methods, moreover it also satisfies forensic requirements. We have discussed in details the techniques of static disk analysis, how to gathering information on a live machine, which live state data and information is all and all accessible on computer.

The goal of this paper is to discuss various techniques used in live and static digital analysis. The rest of the paper is organized as follows. Section II describes literature review. Section III describes the critical review and section IV consists of conclusion and future work in next section.

1.4 Key challenges

The field of live forensic analysis presents new challenges including data snapshots and non-interactive analysis, requiring the development of new data models and user interface designs. When tools are loaded in the RAM to gather and analyze the victim system, some times these tools also affect the memory contents which can misleads the analysis results. This can be overcome by using the appropriate tools and procedures for live digital forensic analysis. Sometimes the requirement is to perform analysis without affecting the functionality of the system so that the entire functionality performed by that system should not be disturbed during performing the digital analysis.

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

1.5 Table of Tools

Sr. No	Tool Name	Op Sys	Purpose/Description	Static/ Live Analysis
1.	Registry Recon	Windows	This tool is used to rebuild the registries of Windows from any place of a hard drive and further it is parsed for the analysis in depth.	Static
2.	SIFT (SANS Investigative Forensics Toolkit)	Ubuntu	SIFT is used to perform digital forensic analysis on different operating system.	Live
3.	EnCase	Windows	This tool is used to gather and analyze memory dump in digital forensic investigation in static mode	Static
4.	Digital Forensics Framework	Windows/ Linux/ Mac OS	During the live and static analysis, DFF is utilized as a development platform and digital investigation tool.	Both
5.	EPRB (Elcomsoft Password Recovery Bundle)	Windows	This toolkit is used to perform digital analysis on encrypted system, password recovery and data decryption.	Live
6.	PTK Forensics (Programmers Toolkit)	LAMP	It is GUI based framework for static and live analysis.	Both
7.	FTK (Forensic Toolkit)	Windows	This tool is used to perform digital analysis and indexing the evidentiary data.	Static
8.	The Coroner's Toolkit	Unix	It is a command line user interface tool to perform forensic analysis on Unix systems.	Both
9.	The Sleuth Kit	Unix/Windows	Toolkit provides GUI and command line interface to perform digital forensic analysis in Unix and windows.	Live
10.	COFEE (Computer online forensic evidence extractor)	Windows	COFEE is used to extract and analyze forensic data lively.	Live
11.	OCFA (Open Computer Forensics Architecture)	Linux	It is a command line interface for distributed computer forensics and it is used to analyze digital media. It is mostly used in digital forensic labs.	Live
12.	OS Forensics	Windows	This tool is used to perform analysis on E-mail, Files, Images and web browsers.	Live
14.	SafeBack	Windows	This tool is used for evidence collection, analysis and for creating backup of evidentiary data in digital media.	Static
15.	Forensic Assistant	Windows	It is used to analyze the activities performed by user on internet like emails, docs and IM and web browsers.	Live
16.	X-Way Forensics	Windows	This tool is used for the general purpose on Win Hex editor used to perform static and live analysis.	Both
17.	CAINE (Computer Aided investigative environment)	Linux	Command line user interface used for distributed and standalone computer forensics.	Both
18.	bulk extractor	Windows, Linux	For the extraction of phone numbers, email addresses, URLs and the other objects which are identified.	Live
19.	IRCR (Incident Response Collection Report)	Windows	Collects live forensics information from the command history, computer, network connection, current processes, opened ports, registry startup information and event logs from system.	Live
20.	Intella	Windows	It is used to process and investigate Email, digital data and Cellphones.	Live
21.	CMAT(Compile Memory Analysis Tool)	Windows	It extracts information from the memory dump and also exposes malware.	Live
22.	WFT (Window Forensic Toolkit)	Windows	Toolkit used to analyze the memory, system information, file/directory timestamp, port number, user information,	Live

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

			and current process and network configurations for digital forensics analysis.	
23.	Responder	Windows	For the robust analysis of Mal ware which includes the disassembly on low level and this tool is also used for the runtime behavior tracing.	Live
24.	FRED(First Responder's Evidence Disk)	Windows	Collects live and volatile forensics information, current processes, opened port number, current logged on users, hidden streams, network configuration, and the files in C: and D: drives.	Live
25.	Memoryze	Windows	It acquires and analyze RAM images which includes the page file on live systems.	Live
26.	Windows SCOPE	Windows	Provides memory acquisition and access to locked computers.	Live
27.	Second Look	Linux	It preserve evidence in volatile memory and also uncover malware.	Live
28.	Volatility Framework	Volatility systems	Toolkit used for the extraction of items from RAM.	Live
29.	Volafox	Mac OS	It extracts digital items from volatile memory.	Live
30.	LiveWire	Windows	The tool used to obtain memory dump and it extracts hard drive data of the network computers and servers.	Live
31.	Network Miner	Windows/Linux	It extracts files, images and other metadata from PCAP files.	Live
32.	Net Intercept	Appliance	It is used to analyze transitory information	Both
33.	Tcp flow	Windows/Mac/Linux	This tool is used for breaking down of flows e.g. sessions as common entities.	Live
34.	WireShark	Windows/Mac/Linux	It is used to captures and analyze packets.	Both
35.	Evidence Eliminator	Windows	It is anti-forensics software which surely deletes the files and claims it as its main job.	Live
36.	NetSleuth	Windows	It can identify and fingerprints network hosts and devices from pcap files which can be captured from Ethernet.	Live
37.	DECAF(Detect and Eliminate Computer Assisted Forensic)	Windows	The user defined actions can be executed automatically using this tool.	Live
38.	HashKeeper	Windows	Database application used for storing file hash signatures.	Static

2 LITERATURE REVIEW

2.1 Review Stage

Cohen *et al.* [1] proposed a rapid response framework named as GRR (Gradual Release of Responsibility) to decrease the investigative effort required per machine. GRR progresses isolated live forensics, by engage in auditing, secrecy issues, and accessible. It delivers a protected and accessible platform to enable forensic analysis solutions. GRR supports automated analysis for a large enterprise data set by executing complex queries in shorter spam of time; thus enhancing the investigative capacity. GRR impose enterprise procedures as it is capable to scan corporate digital assets instantaneously. GRR can help reduce the cost of response and improve quality of evidence.

Mrdovic *et al.* [2] states that live analysis a running system can be used to obtain volatile data to understand of events that had occurred in the past. Running systems are in-capable of being reverse and change their state by making collected evidence invalid. Volatile memory dump can also be used for the analysis of the live data in offline mode. Data can be used from the memory dump; static data creates the virtual machine that can provide good picture of live system when dump was taken. With virtual machine investigator makes interactive sessions without violating evidence integrity. The considered combination of live digital forensic and static analysis offers new possibilities in the virtual environment. In live

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

analysis, system is hibernated before carrying out any examination. It is the best way in order to save volatile memory and state of system and it does not need the change and addition tools in system state. When the system is hibernated, secondary storage image is created and can be used for analysis.

Chan *et al.* [3] state that recent autopsy cyber-forensic techniques may cause disturbance to the evidence gathering process by breaking active network connections and encoded disks. Modern live forensic analysis tools can preserve active state. This proposed framework provides investigators to test the running system without changing its state. It saves the running system state and allows currently working processes like open files, encrypted file system. The proposed framework named as Forenscope can detect secret rootkits, defuse extortions and thus speeds up the investigation process.

Hay *et al.* [4] discussed approaches, the techniques and tools of the live analysis on virtual and real environment. As computer technologies become pervasive, they need supporting digital forensics tools and techniques for efficiently analyzing related system behavior. To investigate the challenges and the progress for the live analysis it is considered very necessary to realize traditional approach of the digital forensics. It implicates the system halting and creating a valid copy of the data for analysis of the storage media. The Static tool searches the storage media for discovering digital evidence. Static analysis results in an incomplete picture of the event. The limiting factors in static analysis pertain to processes shutdown, encrypted data and absence of memory content details.

Whereas the analysis which is done live collects the data from the running system and deals with many inadequacies of the static analysis. There is lot of ways for the live analysis of physical machines during the use of imported utilities, standard user interface and modified system and in the case of VM, the techniques includes interactive logging/replay and the live analysis. Every technique consists of its own advantages and disadvantages. They can also contribute to the live analysis evolution.

Wang *et al.* [5] considered a computer live forensics' model on the basis of physical memory analysis. This model can effectively address lot of challenges which are being faced by live forensics. Authors discussed several issues of credibility of live forensics. Firstly, live forensics calculates the possible creditability which is based on the model of memory analysis, enables validation of live analysis and minimizes impact on collected evidence. Outcomes of live forensics on the evidence, which has calculated, consists of the chance of covering key trace by forensic toolkit and the affects region in digital evidence, authenticity, integrity, verifying consistency rules, repeatability, applicability and fault tolerance.

Khangar *et al.* [6] states that Static analysis is the fundamental approach of digital forensics. It consists of study of data stored on storage media i.e. permanent. When static analysis examined a system, it does not provide complete scenario of event. Hence a VM created from the static data helps in locating evidence. VM facilitates a very simpler way of investigation. Virtualization technology usage in commercial area is growing continuously. So virtual environment needs to be examined itself instead of using virtual environment. Data recovery through using VM files is vertical part. Data recovery is possible in virtual environment but what will be recovered is not predictable. In present era use of virtualization in every organization is very common. Investigation can be done through without violating data collection as evidence since virtual desktop can be made as forensic platform. However virtual environment investigation is simpler than the physical investigation.

Jones [7] proposed a method to improve the integrity and the analytical value of data which is gathered for forensic analysis, a comparison is also provided to identify the limitation in current live forensic techniques. Computer forensic processes have four stages: Collection, analysis, presentation and examination. In Collection stage there is the involvement of location, appropriation and the obtaining data in the forensic manner. Manual and computerized techniques both are involves in examination stage for data identification and extraction. Analysis process uses the applicable data to verify which action has been executed by using the resources of computer. Lastly, reporting shows forensic examiner has gathered information and it will generally take the form of written report. As we see that the dead methodology has full copy of all the data on the storage device i.e. hard disk. This is beneficial and more informative, which is not in hard disk, are present in computers. Computer practitioners have got the response of criminals due to their successes of. For instance there is lot of criminals who use the technique of encryption and undoubtedly they have the accurate copy of encrypted file which is unused by forensic examiner. These files can be opened with Best Crypt program which decrypt data mount file. Such file system can be approached as like another file system when key has been provided to the program. Both encryption and decryption are transparent. As this data is volatile and can be lost with turning off the computers. And other data like decrypted keys which are used for encrypted files can be preserved also in the volatile memory.

Adelstine [8] highlights that information can be extracted from a victim system and this information can be used as evidence in live digital forensic analysis. In dead analysis a static disk image is examined by Digital Forensics and a bit stream copy of a disk is generated when compromised system is powered off. While in live forensics data is collected when victim

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

system is alive. Forensic data collected through live system can give proof which is not obtainable in astatic disk image. Different constraints are used to operate live forensics mainly, the proof collected exposes a dynamic system's snapshot which later on impossible to be reproduced on later dates. Information which is provided by the live system gives a context for disk's data e.g. network connections, running processes, physical memory and process memory and the majority of state items like logged on users, caches and system load, while these are unavailable when system is powered off. In live analysis some hidden processes like rootkits are unavailable but are available in dead analysis. After the collection phase forensic tools are applied on the evidentiary data to perform analysis. Collection of forensic relevant data assists the forensic investigators which produces efficient results and faster response in live digital forensic analysis. When tools are loaded in the RAM to gather and analyze the victim system, these tools some time also effects the memory contents which can misleads the analysis results. This can be overcome by using the appropriate tool and procedures for live digital forensic analysis.

Hay *et al.* [9] Hay et al. [9] shows Xen and virtual introspection (VI) which is termed as VIX tools which is used to put focus on the assessment and test of the computer systems. Here the most vital properties of system akin to acquisition of hard disk and its analysis are available only in volatile memory which can't be recovered by techniques of static analysis. Another approach, in which there is the live study and examination of target systems to expose such volatile data, offers large and considerable risks and challenges to forensic investigators because the techniques of investigation are normally intrusive and it can directly or indirectly affect the system which is under the observation. By the technique of static analysis, such memory cannot be recovered affectively. As this is the real straight forward approach: failure of the defense of system can be observed critically using this ability. Its serious ability to determine how the defense of a system failed and to what extent the affected systems have already been compromised. Using particularly this knowledge, attacks of future can be lessened. Hence, digital forensics' techniques and methods can present such knowledge. Unluckily, due to the introduction of virtualization technologies, digital investigations has become now more complicated and there is more unclearness in the boundaries of the target system.

Alazab *et al.* [10] states that MTF (Master file table) is major part of the NT file system because it contains all the detail of the files and folders. It helps the investigators to fetch the information about the structure and the working of NTFS. MTF contain metadata file which is very important and tells the file system details. The metadata file contain system bootable file ($boot) file. This file is responsible for the booting of the system. This file is static and cannot be changed. The importance of $boot is that it hide the information from hackers and provide the security. If the values of file is changes from its default value then there will no booting of the system. This file contain the information like size, clusters and MFT. So for analyst to perform analysis they should consider one thing very important, that there is a difference between boot sector and backup sector. The major technique used for the analysis is MD5, in which checksum differences reflect that there are some entries that are hidden from the analysis tool.

Casey *et al.* [11] describes that by using FDE (full disk encryption) can be considerably block the digital investigations, which conducts to stopping the access to every digital evidence. Quitting use of evidential system cannot be a technique used satisfactorily, during have the deal with volume encryption or FDE and all the data in results on the device is out-of-the-way for forensic examination. Such challenges can be addressed, for that there will be the requirement for further effective competencies to identify and conserve encryption before plug pulling. Furthermore, in order to provide the better opportunity to digital investigators to obtain the decrypted data in working field, search warrants' preparation is needed by prosecutors with FDE. FDE has disadvantaged earlier investigations, offers directions for assembling the items at the scene of crime that might be beneficial for dealing the data (encrypted), also to perform crime scene forensic acquisitions of live digital forensic systems. Such sort of procedures increases the probabilities of obtaining digital evidence in unencrypted situation or state or detaining a passphrase or encryption key. For drafting, there are some applicants also and performing a search warrants in order to deal with FDE.

Mohamad *et al.* [12] file carving recovers files with unobtainable file system metadata from data storage and in forensics investigation it is very worthwhile. Though, previous carver generation file such as Scalpel and Foremost consider non-fragmented files. Author suggested automatic image and thumbnail carving tool which is known as my Karve. In digital forensics investigation my Karve is worthwhile and evidential information presentation which carve adjoining and fragmented images caused by garbage. myKarve deal with fragmentation and thumbnail issues and it is designed on a new architecture. The thumbnail carving tool tests with the images get from the Internet. myKarve is effective thumbnail carver and automated image compared to the inventive Scalpel.

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

3 CRITICAL REVIEW

3.1 Table

Ref	Area	Merits	Limitations
[1]	Auditing and secrecy issues platform.	It provides cross-platform support for Linux, Mac OS X and Windows clients (agents), and volatility integration for memory analysis. It provides scriptable! I Python console access and basic system time lining features. It also support for asynchronous flows and detailed monitoring of client CPU, memory, I/O usage.	The main limitation of the system is that it requires client server environment and is not feasible for standalone machines.
[2]	Performing static and live digital analysis on virtual environment	It allows static and live combinations of memory dump and highlights rootkits when system is running.	It works on virtual environment which sometimes unable to trace the malware, as some malwares has the property to hide themselves on virtual machine.
[3]	Live forensic techniques and evidence preservations	This framework tested on run time process which don't affect any of the result and process. And it can perform analysis not more than 15 seconds whereas using 125 KB of memory.	It requires transpire as users using more network services, privacy software and non-magnetic storage technologies.
[4]	Challenges of Live analysis	It assists reconfiguring the system to prevent attacks. There are enriched opportunities in digital forensic live analysis arena for R&D according to the both physical as well as virtual machines. Replay ability demonstrates at a pace i.e. arbitrary without giving any alert to user of aimed VM.	There are no repeatable operations. There is lack of user credentials by the investigators for the system which is targeted. System becomes untrustworthy due to alteration of memory. It does not address system integrity completely. Inconsistency leads to some problems like attack detection and automate the reconfiguration.
[5]	Forensics analysis of physical memory	Computer live forensics makes calculating credibility possible. Enables live computer evidence validation. Tool impact on system's data minimized. Consistency verifying technically prevents fake records of investigations.	The live forensics process is not reversibly verifiable. Mixed phases like preservation, analysis, collections etc. is difficult to evaluate its credibility. Due to kernel level modification, unreliable data can be captured by reliable tools.
[6]	Investigating virtual machines in digital analysis	Data recovery is possible by interacting with VM file system. Should have well known structure to handle data.	Data handling improperly may cause irreversible loss of data. Improper handling of data.
[7]	A framework to improve live forensic methodologies	It freezes current state of machine and then during data acquisition, there is no need to make modifications. It gives a guarantee that production of image by this frame work will not have been slurred and kills all those procedures and processes which are not considered important for the system.	Can leads to data modification during the investigation process. Live forensic may leads to damages in evidentiary data due to the factor that program execution normally over writes much data, for example the data which was opened last time and the list of other performed last and recent actions.
[8]	Digital evidence collection	Provides the evidence which is not all available in the static memory dump.	With the continuous increase in size of system, disk data in form of terabytes are no more beneficial and fruitful in term for huge memory storage and number of hours is taken by the imaging. Imaging is impossible and really hard to take on SANs, NAS and RAID arrays. As the disk size increases, in results there is also an increase seen of effort and time for analysis. There are lot of information related to the happening in a running system is vanished. Traditional digital forensics has made efforts to save all (disk) proofs in a state that is unchanging; whereas the

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

			live digital forensic techniques tries and efforts to have a snapshot of computer's state.
[9]	Suit for virtual introspection in digital forensic analysis	Targeted system is logged on by the investigator and he also recorded the logs and there is the creation and deletion of the temporary files. There can be the opening and closing of network connections, updates the history files and there is the addition, queries and modification for the registry entries. Evidence could be hiding due to the installment of root kit by a compromised host like user accounts, open network ports or the files and folders in the computer system. Live analysis attempt can be detected due to the configuration of the system.	It includes the extent of quantification to detect Virtual Introspection by the target system; the VIX suite of tools facilitates recently a brilliant proof of concept for the utilization of VI in digital forensics.
[10]	NTFS file system forensic techniques	Hashing technique provides data integrity and some malicious code lie in boot sector detected.	Up to some extent it can retrieve the data of boot record and not all infections are detected by forensic tools.
[11]	Full disk encryption analysis	Forensic evidence are secured using disk encryption, more relevant data is gathered for analysis.	Digital forensic investigators need to update their skills and procedures of investigations, to perform analysis of encrypted files and volatile data efficiently and effectively.
[12]	Digital evidence preservation and analysis	This system carves non fragmented, linear fragmented images and thumbnail. By using validated headers detects more headers. By using image patterns carves further images and thumbnails. Discarded garbage from fragmented images.	Requires more processing time to scan entire disk image, false carving can misleads the analysis results. It also generates false output while analyzing image files

4 Conclusion

While in the phase of data acquiring in static and live digital analysis, it is required that the memory contents should be consistent with real data, so that appropriate results can be obtained. It is commonly observed that in practically when we run any forensic tool in both static and live analysis to acquire data, it may overwrite the data structure of previously running processes which can lead to inconsistency in evidence which are to be obtained for digital forensic analysis. Hence, the need is to use effective methodology with appropriate tool so that attacks can be detect easily and alteration in memory contents can be minimized. This research produces a brief study of tools and techniques used in live and static digital forensic analysis.

5 Future Work

There are still optimal ways to enhance static and live analysis procedures to produce efficient output. Live and static tools do not produce the required results, which leads to misleading the scalability and suitability of techniques used. So there is a need to choose appropriate methodology which will guide that in which scenario which approach should be adopted. As a future dimension to this, we intend to propose, which technique weather static or live should be adopt for live digital forensic analysis.

References

[1] M.I. Cohen, D. Bilby, and G. Caronni, "Distributed forensics and incident response in the enterprise," *Digital Investigation*, vol. 8, pp. 101-110, 2011.

[2] S. Mrdovic, A. Huseinovi, and E. Zajko, "Combining Static and Live Digital Forensic Analysis in Virtual Environment," *IEEE*, 2009.

[3] E. Chan, S. Venkataraman, F. David, A. Chaugule, and R. Campbell, "Forenscope: A Framework for Live Forensics," *in Proceedings of ACSAC '10*, 2010.

[4] B. Hay, K. Nance, and M. Bishop, "Live Analysis Progress and Challenges," *IEEE Computer and Reliability Societies*, pp.30-37, 2009.

[5] L. Wang, R. Zhang, and S. Zhang, "A Model of Computer Live Forensics Based on Physical Memory Analysis," *in Proceedings of the 1st International Conference on Information Science and Engineering (ICISE)*, 2009.

International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013
ISSN 2229-5518

[6] S. V. Khangar, G. H. R. C. E. Nagpur, and R. V. Dharaskar, "Digital Forensic Investigation for Virtual Machines," *International Journal of Modeling and Optimization*, vol. 2, no. 6, pp. 663–666, Dec. 2012.

[7] R. Jones, "Safer Live Forensic Acquisition," University of Kent at Canterbury, 2007

[8] F. Adelstein, "Live Forensics: Diagnosing Your System without Killing It First," *Communication of the ACM*, 2006 pp.1-6, 2006.

[9] B. Hay,and K. Nance, "Forensics Examination of Volatile System Data Using Virtual Introspection," *ACM SIGOPS Operating Systems Review* 42.3, pp. 74-82, 2008

[10] M. Alazab, S. Venkatraman, and P. Watters, "Digital forensic techniques for static analysis of NTFS images," *Proceedings of ICIT2009, Fourth International Conference on Information Technology, IEEE Xplore*. 2009

[11] E. Casey, G. Fellows, M. Geiger, and G. Stellatos, "The growing impact of full disk encryption on digital forensics," *Digital Investigation*, vol. 8, pp. 129-134, 2011.

[12] K. M. Mohamad, A. Patel, and M. M. Deris, "Carving JPEG Images and Thumbnails Using Image Pattern Matching," *IEEE Symposium on Computers & Informatics*, pp. 78-83, 2011.