OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

COMPARATIVE ANALYSIS OF FREEWARE FOR FLASH DRIVE DATA SANITIZATION

Deepika Chauhan[1], Dr. Pratosh Bansal[2]
IT, IET DAVV, Indore, Madhya Pradesh, India[1]
Professor, IT, IET DAVV, Indore, Madhya Pradesh, India[2]
chauhandeepika522@gmail.com[1], pratosh@hotmail.com[2]

Abstract: **Demand of computer forensics increased because the numbers of computer crimes have been increased and committed daily. Technologies and Sciences have become the backbone of today's life. If any security system has been breached or crime has been practiced using computer or electronic devices then need for computer forensic gets generated for investigation and justice purpose. There has been an increase in concern for privacy and information security, radically in the light of technological advances and the practical increase in type of electronic communication. Hard disk drives (HDDs), Compact Disks (CDs), and Universal Serial Bus (USB) drives, etc. are mostly used information storage devices, for in support to almost all aspects relative to technology based life. Magnetic Storage devices are the most commonly targeted media for investigation and diagnosis purpose. As the users are now aware about the forensics tools today, they try to find out or access confidential information. In this paper, we discuss about some anti-forensic techniques/ methods which are performed on the digital devices. Anti-forensics is the collection of methods used against digital forensics. This research work focus on a significant anti-forensic technique *"Data Sanitization"* to delete or remove data completely from flash drives to test drive against criteria such as computation time required, efficiency of algorithm, tool performance and amount of data recovered.**

Keywords: *Data Sanitization, Investigation, Disk Wipe, Secure Eraser, Anti-forensics.*

---∴∴∴---

I INTRODUCTION

In modern era, *Forensic Science* is used to make the legal procedure more accurate and genuine by applying it in the investigation process. Proper use of methodologies and algorithms makes this approach more scientific. An important scientific approach can be developed by combining both, to solve criminal investigations [1, 2]. It has been derived from several branches of sciences like physics, chemistry and biology using known and focused approach for facts collection [2]. It has become a significant part of the judicial structure due to ample scope of achievement and precision. Collecting, preserving and analyzing the scientific proof obtained during investigation, is the application of science in judicial system [3, 4]. It is famous for research, identification and analysis of any event /document/scene identification [5]. The facts obtained from these domains play an important role in judiciary and law to identify the reason behind any criminal act and the method used for that events to happen which becomes case study for analyzing another cases [6,7].

Forensic science is also the field of investigation and security which helps to solve several criminal cases [8, 9]. It has become a very important part of several criminal activities as they serve a service of determining the scientific fact behind that event through the scientific knowledge and fact obtained from the different branches of the forensics [10, 11, 12]. The documents obtained from the forensics play vital role in the investigation. The testimony generated is the truly trusted component for any criminal activity. The professionals are not concerned with the output of the study but they rely on the facts generated during the analysis [12].

Moreover, *Forensic scientist* performs all the analysis required at the crime scene to obtain the evidence. Generally they go through the physical and chemical analysis of the devices obtained at the crime sight [13]. For investigation they are using different techniques like microscopic examination technique, complex instruments,

mathematical principles, algorithms, scientific principles, case studies and reference literatures for the analysis of digital evidence and identification of the entities and their characteristics [14].

Forensic researchers burrow each earthly and concoction examinations on physical purpose of correlation got by offense parade agents and wrath officers at the infringing upon of the law scene [14, 15]. These careful authorities handle minute inspecting procedures, comparatively radical instruments, scientific standards, exhaustive standards, and tribute writing to investigate proof on tossed in one part with every bit of activity and companionless qualities. Majority of forensic scientists are doing their jobs in specially designed laboratories which are designed for the purpose of obtaining and generating the facts about the devices and entities [15]. These laboratories are equipped with all the necessary tools such as hardware, software, advanced machinery which is required for the analysis. Forensic scientists work for local states, federal laws, enforcement bodies, independent forensic science consultants, government, private laboratories and the hospitals [15]

II DIGITAL FORENSICS

Digital Forensics are the techniques of learning of rendering and analysis of digital devices using combination of different domain of technologies/software and hardware components. Through this we obtain some relevant facts about the event using minicomputers [15]. Now, Digital forensics investigation plays a very vital role in securing the modern world. As the world is filled with lots of digital devices, the forensic investigation has plenty of applications in today's investigations [15].

The facts obtained from the degree of the investigation goes through the device is distributed into all the sub-branches to refer the mutual references for the digital device involved. Microcomputer forensic become an important part for the investigation now. Forensic reference experiments and mobile stylistic allegory forensics can be used for investigation. For doing this imaging of device can be done and examination of these imaging of device can be done to obtain the fair results.

Laptop forensics is that the heed of assembling, analyzing and coverage on digital flea in ear in a as a matter of fact approach that's wrongfully allowable. It is periodic utilized in the detection and delay of misdemeanor and in entire clash wherever principle is bolstering on digitally. Microcomputer forensics follows an analogous rule of thumb to arbitrary forensic disciplines, and faces evocative problems. There are few areas of infraction or clash wherever microcomputer forensics cut back not to be applied. Enforcement agencies are in the earliest and heaviest users of microcomputer forensics and by its own nature have truly been at the leading edge of developments within the field.

III PROCESS OF DIGITAL FORENSICS

Digital forensic investigation process majorly consists of following phases [17].

1) ***Identification:*** Basically, It is a combination of three processes which encompasses validity of incident, generate list of operations required and generate flow of actions to be performed depending on knowledge.
2) ***Authorization:*** In this phase, an approval has been taken for the investigation to be done.
3) ***Preparation:*** In this phase, identify the required tools, generate steps to be followed, create investigation plan, identification of operation required and task allocations.
4) ***Securing and evaluating the scene:*** Under this, investigate the entities or devices and characters at the sight of crime and find out more possibilities, safe equipment, recognize and protect proofs by conducting interview.
5) ***Documentation of the scene:*** This is a very important phase in which, Information gathered from above mentioned steps are converted into documented proof by creating a record of documents which consists of photographs, notes, conditions, location information of devices, components that are removed or not, sealed and unseal able component, evidence bags and other facts.
6) ***Evidence collection:*** In this phase, collect all the evidence present physically such as digital device, analog evidence such as password, hand written notes, printouts, computer manual or any other referral physical entity related to crime.
7) ***Packaging, transportation and storage:*** After the evidence collection, generate feasible conditions for the evidence collected so that no alteration of information can be done such as protection of media and equipment during transfer, avoiding extreme pressure or exposure to conditions unfavorable for the device, effect of vibrations, magnetic source, elasticity etc. and maintenance procedure for storage and reception, chain of custody, copies of evidence and inventory for storage of media.
8) ***Initial inspection:*** This phase is the combination of several tasks such as device identification, tool selection, algorithm or process selection and expected outcomes.
9) ***Forensic imaging and copying:*** Under this process, physically remove hard drive from computer and generate a digital image for investigation and capture its behavior which can be done with many software tools available in the market. It is a combination of physical and logical acquisition.

10) ***Forensic examination and analysis:*** In this phase we are using different forensic science tools and techniques for processing which include creation of cryptographic hash values and its filtration with the help of hash libraries, viewing and exporting file and compound files (e.g. email) expansion, metadata extraction, indexing and searching.
11) ***Report and Presentation:*** In this phase we finally document the proofs obtained during analysis in which we cover procedure of investigation, findings, bookmarks, log files, notes. We generate the final conclusion based on the facts for further processing in court [18].

Figure 1 depicts a typical process of Digital forensic investigation which includes the major following four phases:

1. Identification
2. Acquisition
3. Analysis.
4. Presentation

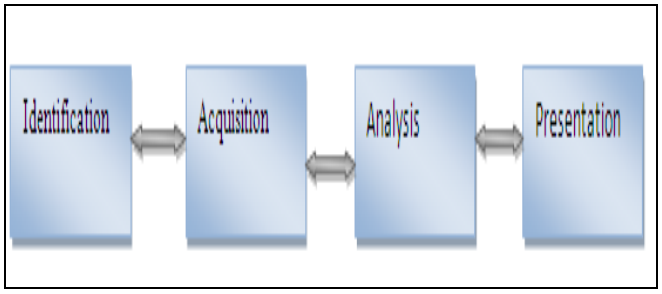

Figure 1: Process of Digital Forensic [18,19]

IV DATA SANITIZATION

Data sanitization lies under Anti- Forensic methods which either erases the complete records of information or displays masked information to protect it from unauthorized access. It is the procedure of purposely, for all time, and irreversibly expelling or the information put away on a memory gadget. A gadget that has been effectively disinfected has no leftover information notwithstanding when information recuperation is endeavored with cutting edge measurable instruments. Sanitization forms incorporate utilizing a product utility that totally deletes the information, a different equipment gadget that interfaces with the gadget being cleaned and eradicates the information, as well as an instrument that physically crushes the gadget so its information can't be recouped [18, 20]. Sanitization procedures are generally utilized by Government bodies where there is a need to keep up mystery among the authoritative records. Commonly they utilize a depended procedure, known as *Data Redaction* which manages altering substance or disguising the delicate data in the first record rather. The strategy utilizes shrewd and savvy procedures that make the common crowd unconscious of the data however on watchful examination the mystery piece could be uncovered [20]. Data sanitization can be defined as: *"Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data and even advanced forensic tools should not ever be able recover erased data. "*

V NEED FOR DATA SANITIZATION

Data sanitization is very important. The following are the few important examples which are helpful in understanding the need of data sanitization:

(a). Selling and purchasing of digital devices.
(b). Pass ownership of treasure from one to a different course.
(c). When you wish to finish up business.
(d). Replacements or updating of Hard disk warranty.
(e). Wipe out records completely from digital devices to reuse.
(f). For either reusing or reallocating the services rendered by cloud.

VI DATA SANITIZATION TECHNIQUES

Data sanitization techniques are the methods which are used to destruct, wipe or delete data permanently from any memory device. They are sometimes referred as wiping standards which are different for different countries which are followed by some specific pattern or steps to make data unrecoverable [20, 21, 22].

Following Data Sanitization Techniques have been proposed for removing content from hard disk drive.

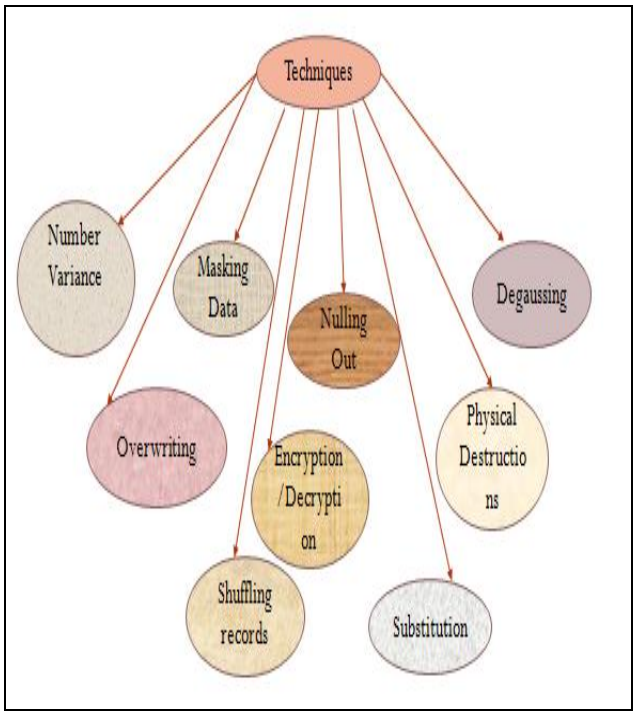

Figure 2: Data Sanitization Techniques [20]

1. Nulling out
2. Masking data
3. Substitution
4. Shuffling records
5. Number variance
6. Encryption/decryption
7. Degaussing
8. Physical destruction
9. Overwriting.

VII DESIGNING ISSUES IN DATA SANITIZATION

Before applying data sanitization over any memory device, we have to determine the different parameters which might produce issues during the sanitization. Here we discuss about some issue which we carried in mind before starting the sanitization over any device:

a) Recognition of level of confidence

Different disk sanitization methods offer distinct levels from higher to lower

- Highest confidence-physical destruction
- zeroing media entirely
- zeroing the affected record and file
- Lowest confidence-Erasing the affected file and file record.

b) Low level search

This is needed to verify that data is removed successfully or not.

c) Security

Complete sanitization is practically not possible so if there exists, a chance of residual which may contain some sensitive information.

d) Number of passes

Number of passes of an algorithm required to complete the sanitization, is an intricate matter, because with the increase in number of passes the probability of damage of media happen.

e) Time

How much time is required to run any algorithm?

f) Damage

There may be a possibility of permanent deformation of storage media.

g) Cost

With every increase in number of passes, eventually the cost increases.

h) Security level

Evaluating, sensitivity and security level of the stored information.

i) Type of Sanitization

To choose a suitable media sanitization type on the basis of category.

j) Sanitization method

To choose, an appropriate media sanitization method for the media [20].

VIII DATA SANITIZATION TOOLS

Data sanitization tools are sometimes referred to as data destructor/Erasers or wipers. These are the software based utilities which we are using for the sanitization of data. These are available in different formats and use different algorithms for the sanitization. They generally make use of the principle of overwriting the data. They are used to completely delete data from any memory device. When we delete any file or remove it from the recycle bin, we actually delete only the reference of that file present in the allocation table of system's file system, not the actual file which can be easily recovered by some recovery tools available in market. *Data destructors* are the software based methods which utilize independent or combination of techniques defined for the data removal which permanently delete data from any memory device.

Mainly, five tools are considered as the data sanitization tools to perform experimental analysis. List of all those tools are cited below:

1) CCEraser
2) Hardwipe
3) SecureEraser
4) Diskwipe
5) KillDisk

IX EXPERIMENTAL SETUP

The experimental work has been performed by using 03 steps:

1. Installation

Installations for all sanitization tools have been performed. The comparatives for specification needed to install and the features provided or supported by the tools are available in the *Table 1* and *Table 2* respectively

2. Sample data

Variable size of sample data for instances (500MegaBytes, 100 MegaBytes, 1500 MegaBytes, 2000 MegaBytes, and 2500 MegaBytes) have been generated with varying files formats and varying memory sizes i.e. .jpg/.jpeg, .mp3/.mp4, .doc/.docx, and .txt etc.

3. Verification Sample data integrity

Integrity of every sample data has been properly verified and MD5 has been calculated using in important tool known as ImageUSB and verification have been done for normal and .bin data sample.

Table 1: Comparitive Study Of Data Sanitization Tools On The Basis Of Specification

SPECIFICATIOS	*CCERASER*	*HARDWIPE*	*SECURE ERASER*	*DISKWIPE*	*KILL DISK*
Type of Operating System	Windows	Windows	Windows/Mac/Unix	Windows	Windows/Linux
Types of File Systems	Almost all	Almost all	Almost all	Almost all	Almost all
Types of license	Available in Open source	Available in Open source or Professional or Commercial	Available in Open source or Professional	Available in Open source or Professional	Freely available
Types of File supported	Almost all	Almost all	Almost all	Almost all	
Availability for Files	.exe file	.zip file	.zip file	.exe file	.exe file
Size of the tool	Information not available	Information not available	4.7MegaBytes	1.05MegaBytes	8 MegaBytes
Versions available	Information not available	v5.1.3	v5	v1.7	v10.01

Table 2: Comparative Study Of Data Sanitization Tools On The Basis of Features

FEATURES	*CCERASER*	*HARDWIPE*	*SECURE ERASER*	*DISKWIPE*	*KILL DISK*
Number of Algorithms used	4 Nos.	6 Nos.	3 Nos.	7 Nos.	8 Nos.
Portability of the Tool	Portable	Portable	Portable	Portable	Portable
Supporting the Devices	All USBs	All USB and/or SD Cards	All USB and/or HARDDISK	All USB/HARDDISK/SD Card/ other Memory Storage	Linux/ Windows
Residue feature	Information not Available	Information not Available	Information not Available	Information not Available	Information not Available
Used Method	Method of Overwriting	Method of Overwriting	Method of Overwriting	Method of Overwriting	Method of Overwriting
Availability of Free Space	No space	Totally Clean	Totally Clean	Not mentioned clearly	Totally Clean
Verification of Data	Information not Available	Not done	Not done	Done	Not done
Feature of Usability	Information not Available	Useful for File, Folder, Registry, Recycle-bin etc.	Useful for File, Folder, Registry, Recycle-bin etc.	Information not Available	Multiple feature of Disk Eraser
Requirement of Installation	Yes	No	Yes	No	Both

X SETUP TO EXPERIMENTAL ANALYSIS

Experimental Analysis have been performed along with Data rates and also with computation time. Below we are presenting a diagnosis of each tool.Figure 3.1, 3.2, 3.3, 3.4 and 3.5 show the results generated for the sanitization of the data used for test using the 05 tools called (a) CCEraser, (b) Secure Eraser, (c) Hard Wipe, (d) Kill Disk and (e) DiskWipe respectively. The vertical axis displays the variation in data rates in bps (bits per second) and the horizontal axis shows the various types of algorithms performed on the same tools.

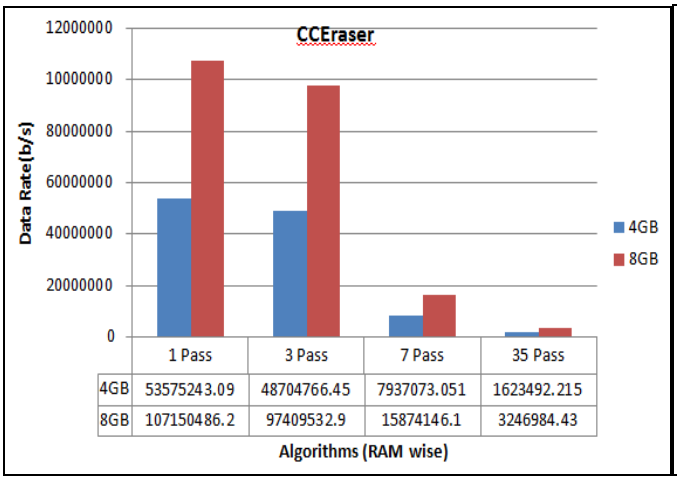

Figure 3.1: CCEraser Data Rate.

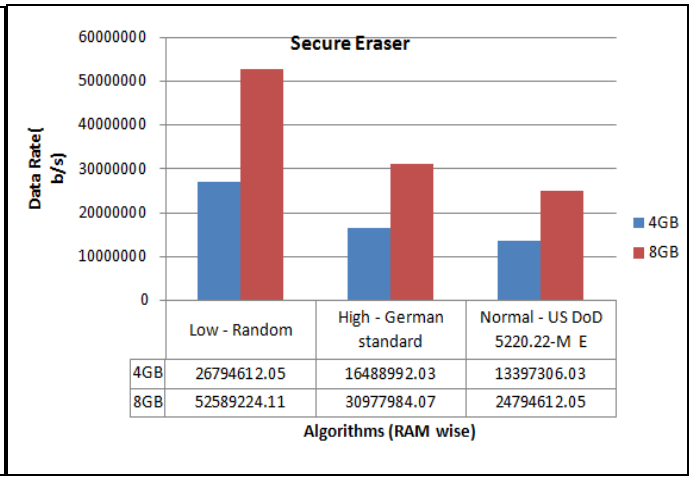

Figure 3.2: Data Rate of Secure Eraser.

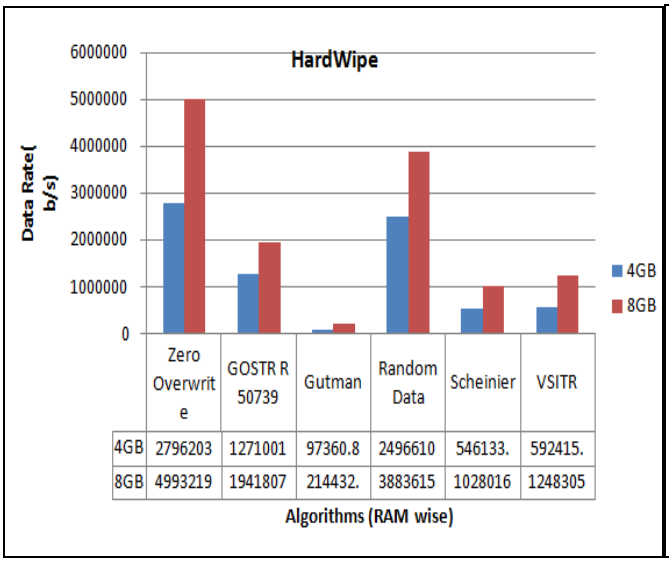

Figure 3.3: HardWipe Data Rate.

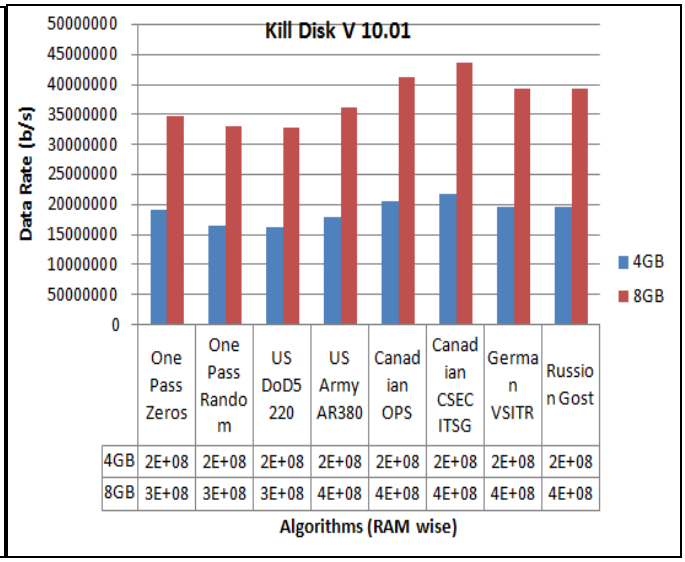

Figure 3.4: Kill Disk Data Rate.

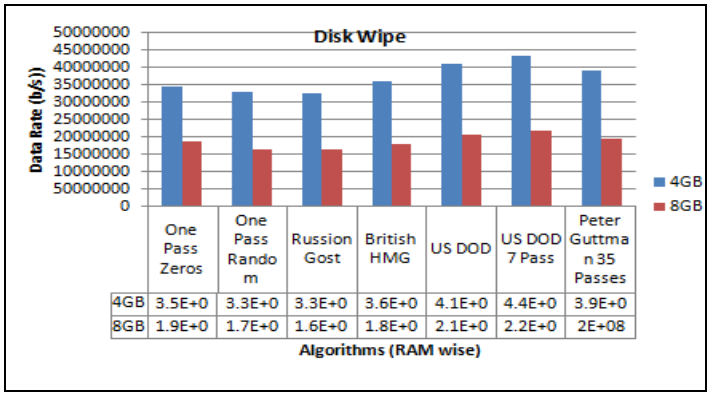

Figure 3.5: DiskWipe Data Rate

Similarly, figure 4.1, 4.2, 4.3, 4.4, & 4.5 displays computation time the analysis by the same tools called *(a) CCEraser, (b) Secure Eraser, (c) Hard Wipe, (d) Kill Disk* and *(e) DiskWipe*, respectively.

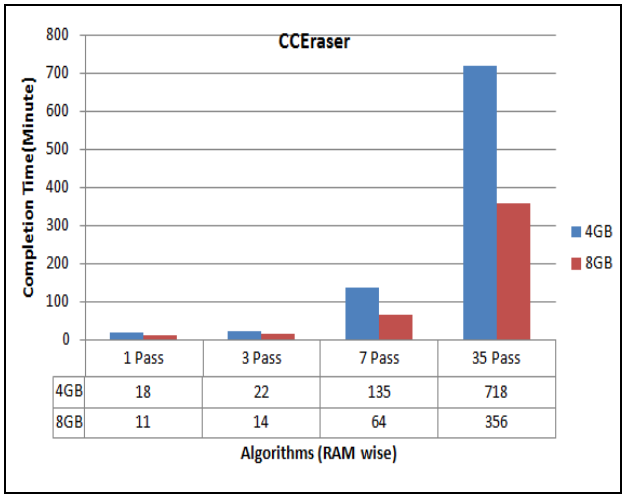

Figure 4.1: Computation Time taken by CCEraser.

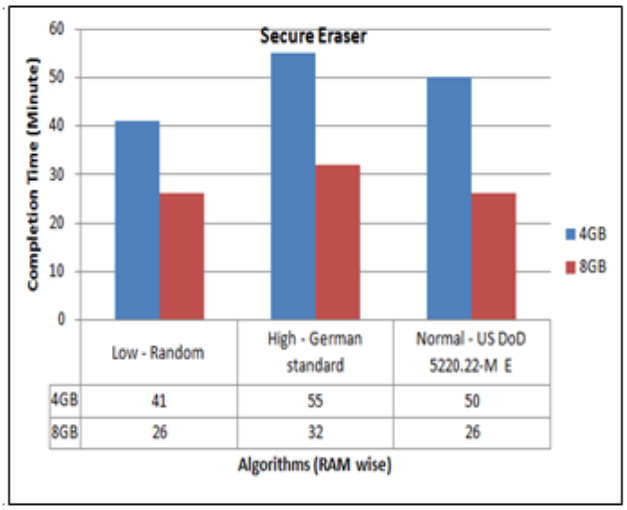

Figure 4.2: Computation Time taken by Secure Eraser

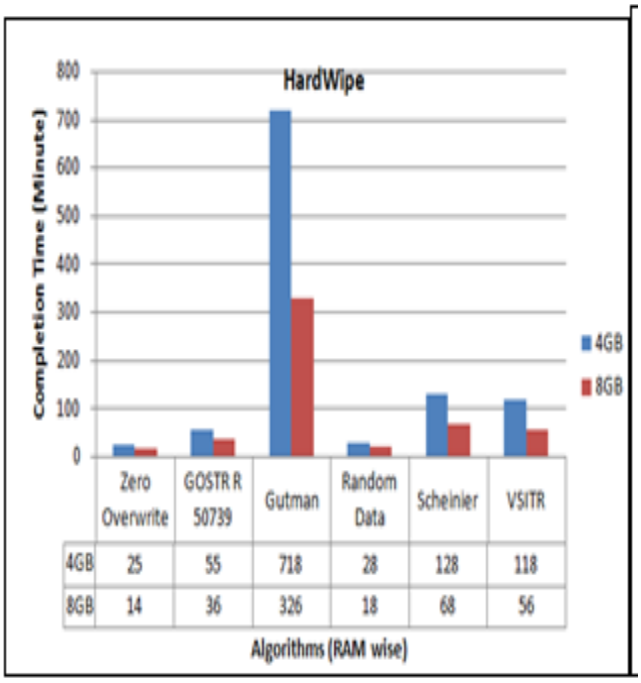

Figure 4.3: Computation Time taken by HardWipe.

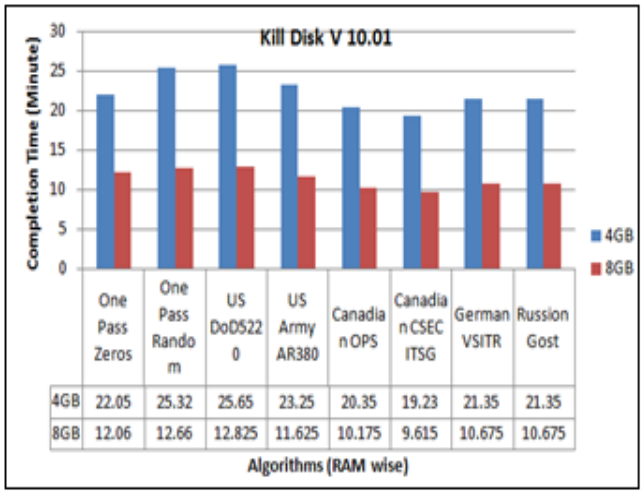

Figure 4.4: Computation Time taken by Kill Disk

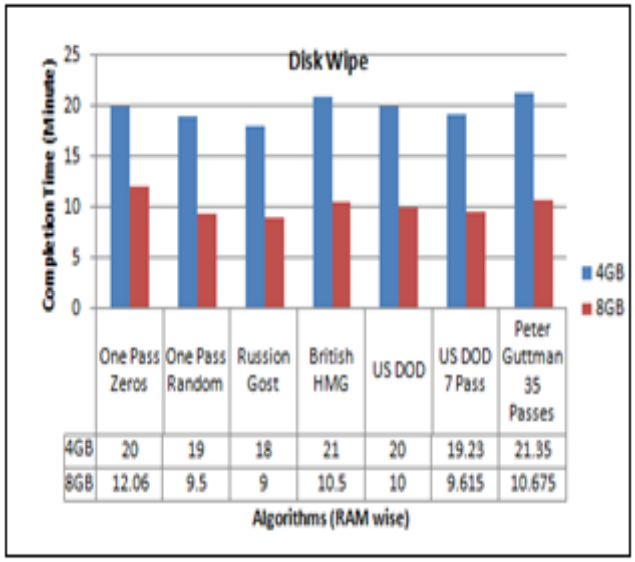

Figure 4.5: Computation Time taken by Disk Wipe.

XI CONCLUSION

Study shows that data sanitization is among the significant tasks of computer forensics that offer diverse levels of isolation and protection of data after its utilization. Computer Forensics acts as a significant method to preserve the security in any type of confidential work. Using recovery tools, international enemies and terrorists may recover the sensitive content using from the damaged HDDs or other memory storage devices.

To protect the information by such kinds of events and to provide a protected atmosphere for avoiding recovery of data, data sanitization can be used. This research work was started to investigate the requirement for data sanitization and spot the most appropriate tool to achieve the process. Five different sanitization tools has been considered during the whole research and variable data sizes (500 MB, 100MB, 1500MB, 2000 MB, 2500MB) samples has been analyzed with all respective algorithms. For ensuring the integrity

confirmation, the work also utilized MD5 method and validates the digest value for ISO file using ImageUSB. The whole study made some observations which are listed below:

1. Analysis for CCEraser tool:

a) There are four diverse algorithms that are used for sanitization purpose and their classification is done on the basis of passes.
b) To achieve accuracy the number of passes may vary up to minimum one pass and maximum thirty five passes. The data rate decreases and computation time increases with improvement into passes.
c) Though, with high pass value, overhead is also increased, but it also increases the security level and trustworthy process of sanitization.
Whole process is performed on 4GigaBytes and 8GigaBytes RAM. The observation indicates that the configuration with 8GigaBytes RAM helps in system performance amplification.

2. Analysis for Secure Eraser tool:

a) Secure Eraser tool is connected with three different algorithms based on sanitization algorithms.
b) In Normal DOD, Poor Data rates have been noticed but in case of German and low category method for sanitization, similar kinds of data rates have been recorded.
c) Almost all algorithms for sanitization showed similar computation time.
Whole process is performed on 4GigaBytes and 8GigaBytes RAM. The observation indicates that the configuration with 8GigaBytes RAM helps in system performance amplification.

3. Analysis for HardWipe tool:

a) To clean the existing disk, six techniques are presented based on various sanitization algorithms.
b) For Guttman method, Poor Data rates and much computational time were recorded but for other methods similar data rates have been recorded.
d) Whole process is performed on 4GigaBytes and 8GigaBytes RAM. The observation indicates that the configuration with 8GigaBytes RAM helps in system performance amplification.

4.Analysis for KillDisk tool:

a) Based on different sanitization algorithm, various methods have been proposed to clean the existing disk.
b) In terms of computation time and data rate, similar results have been recorded.
Whole process is performed on 4GigaBytes and 8GigaBytes RAM. The observation indicates that the configuration with 8GigaBytes RAM helps in system performance amplification

5.Analysis for DiskWipe tool:

a) There are eight methods that are proposed on the basis of various sanitization algorithms to clean the existing disk.
b) In terms of computation time and data rate, similar results have been recorded.
c) The whole process is performed for 4GB and 8GB RAM. The observation indicates that 8GB RAM configuration helps to amplify the system performance.

6.No changes has been observed in MD5 and SHA-1 during continuous calculation and verification of MD5 on USB Drive after and before applying to disc wipe out; This clearly indicates that none damages have been encountered during zero(0) and one(1) pass algorithms.

7. In respect of experiencing variousl tools with the enhancement of passes, raise in data rate is recorded.

8.Afterwards, with respect to passes, computation time is also enhanced.

9. *Kill disk* performs well for data rate in contrast to other tools.

10 *Hardwipe* and *CCleaner* give very poor performance under computation time.

11 For data rate, *Secure Eraser* and *Kill-Disk* provides excellence result.

Therefore, the entire research work deduce that before scraping or reselling the memory devices, Data sanitization should be used all the time. It may be unsafe for security and privacy reason to avoid this procedure.

REFERENCES

[1] Chris Pogue, Cory Altheide and Todd Haverkos. “Unix & Linux Forensic Analysis Toolkit”, edition-first published by Syngress Publishing, Inc. & Elsevier, Inc.,2008, Burlington-USA.
[2] Brian Carrier. “File System and Forensic Analysis”, published by Pearson Education, Inc, 2005, New Joursey-USA.
[3] Paul Bakker. "Search Tools, Indexed Searching in Forensic Images", published by Sleuth Kit Informer 2004. Available on http://www.sleuthkit.org/informer /sleuthkit-informer-16.html#search.
[4] Simson L. Garfinkel. “Digital forensics research: The next 10 years”, published by Digital Forensic Research Workshop-Elsevier Ltd.
[5] Blog: ”Access Data. Forensic toolkit overview”, http://www.accessdata.com/Product04_Overview.htm?ProductNum¼04; 2005.
[6] Saltzer Jerome H and Frans Kaashoek. ”Principles of Computer System Design: an Introduction”, 2009.
[7] Nicole Beebe. “Digital Forensic Research: The Good, the Bad And The Unaddressed”.
[8] T. Abraham, R. Kling and O. de Vel. “Investigation profile analysis with computer forensic log data using attribute generalization” processing of 15th Australian joint conference on arterial intelligence,2002.

[9] E. Huebner, D. Bem, F. Henskens and M.Wallis. "Persistent systems techniques in forensic acquisition of memory, Digital Investigation" vol. 4(3-4), pp. 129–137, 2007.
[10] G. Dorn, C. Marberry, S. Conrad and P. Craiger. "Analyzing the impact of a virtual machine on a host machine, in Advances in Digital Forensics", V, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 69–81, 2009.
[11] Nance, K, and D J Ryan. "Legal Aspects of Digital Forensics: A Research Agenda", 2011 44th Hawaii International Conference on System Sciences, 2011.
[12] K. Bailey and K. Curran. An evaluation of image based steganography methods, International Journal of Digital Evidence, vol. 2(2), 2003.
[13] N. Beebe and J. Clark. A hierarchical, objectives-based framework for the digital investigations process, Digital Investigation, vol. 2(2), pp. 147–167, 2005.
[14] Deok-Soo Kim. "Piecewise Power Basis Conversion of Dynamic B-Spline Curves and Surfaces", Advances in Geometric Modeling, 01/29/2004.
[15] Richard Austin (2007). "Digital forensics" available at www.snia.org /1/9/2015.
[16] Chuck Moozakis (Oct 11, 2013). "Network Forensic", available at: http://searchsecurity.techtarget.com/ definition / network-forensics
[17] YunusYusoff, Roslan Ismail and Zainuddin Hassan. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011 "common phases of computer forensics investigation models" available at http://airccse.org /journal/jcsit/0611csit02.pdf. 25/11/2015.
[18] "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" available at https://www.ncjrs.gov/ pdffiles1/nij/199408.pdf 1/12/2015.
[19] A Net 2000 Ltd. "Data Sanitization" available at (accessed on 10/12/2015): http://www.orafaq.com/papers/data_sanitization.pdf
[20] Net 2000 Ltd. "Techniques of sanitization" available at (accessed on 4/9/2015): www.datamasker.com
[21] Kate Holmes (26 FEB, 2016) "Understanding the Impact of Anti-Forensics Techniques" available at: http://www.ftitechnology.com/resources/blog/understand ing-impact-anti-forensics-techniques