Effectiveness of OSForensic in Digital Forensic Investigation to Curb cybercrime

Bandr Siraj Fakiha

Associate Professor, Department of Medical Health services, Faculty of Health Sciences , Umm Al-QuraUniversity, K.S.A.

Abstract

With the rapid development and higher level of dependence on new information and technology by various organizations across the world, cybercrime issues are increasing, and there are no technologies that seem flawless in combatting the issue. The use of concepts relating to digital forensic investigation of criminal activities and digital forensics will, therefore, tackle the problem with finding digital evidence in cybercrimes. OSForensics is one of the various digital forensic investigation tools that allows the use of Hash Sets for identifying known safe files in program and operating system files. The tool is essential for identifying suspected files like Trojans, viruses, and hacker scripts. The problem presented in this paper, therefore, entails utilizing combinations of digital forensic investigation of criminal activities and investigation concepts. The paper seeks to establish the effectiveness of OSForensic in Digital Forensic Investigation to curb cybercrime. That is, the capabilities of OSForensics and the accuracy of OSForensics with regards to retrieving and analyzing data from a hard drive in order to investigate and curb cybercrime at the workplace. The researcher investigated a case in which a company security had been threatened by an employee whose contract had recently been terminated. The company suspected that this employee had some serious pictures, locations, and employee details belong to company. The image of the employee's personal flash was sent to the researcher to help initiate the investigation using OSForensicssoftware so as to establish any evidence that the employee still had pictures, locations, and employee details belong to company. In overall, OSForensic was able to identify company details that the employee was having. The research was able to identify sensitive information about the company that the suspect was having, including the names of the employees, images, company system structure and what seemed to be their respective identification numbers.

Keywords: *OSForensics; Cybercrime; Digital Forensic; Investigation*

Introduction

Digital forensics refers to walking back through incidents in computer systems to investigate crimes or to map out digital assets [3]. Kishore et al. [5] define data analytics as collecting, aggregating, and analysis tools for the detection of threats and monitoring security. Information Security, as [4]asserts, encompasses other issues such as access control, risk assessment, malicious software, and incident investigation. A new tool is provided that combines digital forensic of illegal activities and digital forensic investigation concepts to determine cybercrime patterns, find motives for cybercrime, and for keeping score of the number of cybercrimes that occur in a given period. Moreover, digital forensic investigations inquire about questionable and unfamiliar activities in the digital world [15]. Digital forensics, therefore, is useful in understanding attacker behaviors that get done through the collection and analysis of status information and logs [11]. Losavio et al. [8]explain that attacks mostly occur as a result of unawareness. Naskar, Malviya, and Chakraborty [10] note that through the unawareness of users, systems become more prone to cybercrime, which almost always occurs without notice. Forensic process is one that is done in steps, and the number of steps depends on the forensic type[12]. Mostly, however, the first step in digital forensics is the identification of potential data sources and the acquisition of data that is useful in forensics from these sources [20]. Some of

the primary data sources are routers, storage media, desktops, and cell phones, etcetera[2]. Plans are required for getting the data from the primary data sources for which priorities will be provided based on the data's volatility, importance, and the amount of effort for collecting the data. The investigation process follows the steps of extracting relevant information pieces, analysis for drawing conclusions, and reporting for preparing and presenting the outcome of the analysis step. Some of the types of digital forensics include computer forensics, firewall forensics, database forensics, and live systems forensics, and software forensics, among others. Of the said types, computer forensics is most essential as it involves analyzing and investigating for the collection and preservation of evidence [18].

The present research employed the forensic investigation techniques used in OSForensics. The hash sets for identifying known safe files in program and operating system files have been used for the project. The OSForensics is available commercially as a digital investigation suite for Windows. This tool retails at around $995 USD with 12-months support and updates[13]. The suite is capable of mining forensic evidence from computers and implementing file searches and indexing. OSForensic is mainly used in cybercrime investigations and can be useful in initiation of investigations. It used to create a new case and fill case details. For example, we can browse for the USB image to create the hash for the image; this helps in checking if the hash is changed or not after collection of evidence[19]. OSForensic scans the image to check the recent activities such as access website, recent downloads and USB drives. The problem presented in this paper, therefore, entails utilizing combinations of digital forensic investigation of criminal activities and investigation concepts. The problem issue for this project is that presently, cybercrime issues are increasing, and there are no technologies that seem flawless in combatting the issue. The use of concepts relating to digital forensic investigation of criminal activities and digital forensics will, therefore, tackle the problem with finding digital evidence in cybercrimes. The paper seeks to establish the effectiveness of OSForensic in Digital Forensic Investigation to curb cybercrime.

Materials and Methods

The researcher initially researched more on OSForensics so as to determine the extend in which it works and found out that numerous options are available for the investigator to use in OSForensics free edition.

Based on the fact that there are numerous options available for the OSForensics, and since the research had limited number of researchers and time, the forensic investigation was narrowed down to USB Registry Activity. The researcher investigated a case in which a company security had been threatened. The company had just terminated an employee that was working in their security team. They suspect that this employee had some serious pictures, locations, and employee details belong to company. The image of the employee's personal flash was sent to the researcher to help initiate the investigation so as to establish any evidence that the employee still have serious pictures, locations, and employee details that belong to the company.The researcher started forensic investigation with the USB image, then opened VM ware and created a folder for the study investigation and then started the investigation using OSForensic tool. A new case was then created and named the case with Investigating G2 Image filled case details and then browsed for the USB image. The researcher then took the hash for the Image for verification.Subsequently, the researcher created SHA1 hash and saved the result in notepad.The image was then selected after it had been extracted. The image was then added and new folders established. The folders were used to investigate all the deleted files.

The investigation revealed some interesting files; for instance, Marta contained pass codes. The researcher also found another text file called "name" that had a list of suspected employees' names and also found the location.Sensitive information about the company with file called workstation was also established. What seems to be the company network diagram was also found. The researcher also found what appeared as employees ID from the file "Football Information":

Result and Discussion

OSForensics was capable to create hashes and hash sets for different files, one single text string, or a whole volume with SHA-1, CRC32, MD5 or SHA-256 hashes.

It was possible for the investigator to calculate the hash of the file, the individual text string or volume and consequently compare it to a hash value which is well known. The create/verify hash function was applied to hash different folders and files on a forensic image. As shown in the figure below, OSForensics has the general ability to hash the individual drives and folders/files on the respective drive. The time for completing the hash varied, depending upon the drive that was being hashed and the file size.

In overall, Forensics was able to identify company details that the employee was having. The research was able to identify sensitive information about the company that the suspected employee was having, including the names of the employees and what seemed to be their respective identification numbers.

According to Hidayat et al. [1]OSForensics is a digital investigation tool that allows the use of Hash Sets for identifying known safe files in program and operating system files. Hidayat et al. [1] further explain that this tool is essential for identifying suspected files like Trojans, viruses, and hacker scripts. Among other benefits, OSForensics allows for faster extraction of forensic data from computers and reduces the need for further time-consuming analysis.

The tool can detect suspicious activities and files employing hash matching, drive signature assessments, and binary and memory data [7]. It finds hidden sectors in the hard disks, looks through volume shadow copies to analyze the previous versions of files and validates file matches with MD5 (message-digest 5), SHA-256 (secure hash algorithm 256), and SHA1 hashes [18]. It also has disk drive imaging feature to store the drive content replicas. In addition, RAID (Redundant Array of Independent Disks) arrays are accomplished from each disk image with the help of this tool.

According to Hidayatet. al. [1] and as has been established in the present paper, OSforensics software restores deleted data effectively, particularly data removed by the perpetrators. In their study, Hidayatet. al. [1] carried a four-phase comparative analysis of OSforensics. They made the comparison with Disk Genius, GetDataBack and Diskdigger forensic toolkits for data retrieval on Windows 8 Operating System. Analysis began with formatting the flash drive and then filling out data on the flash drive. All the data in the flash drive was deleted and the recycle bin emptied. The digital forensic toolkits were then used for data recovery. The OSforensics kit recovered the deleted data precisely compared to Disk Genius, GetDataBack and Diskdigger.

Lahaie[6] also carried out a four-phase forensic process on a 32GB USB drive using the OSForensics tool. The tool was used to create an MD5 hash of the drive before and after the data acquisition phase. The researcher applied a USB write-blocking registry tweak to ensure that data could not be altered before connecting the USB to the computer; implying that the disk is forensically sound. The OSForensics locked the USB further, producing matching MD5 hashes before and after the acquisition, indicating that OSForensics is forensically effective in the field of digital forensics.

However, Hidayat et al. [1] acknowledges that digital forensic investigators follow specific stages and measures when working on an incidence. For that reason, investigator is likened to tools because they act as tools in tracking and persecuting criminals. Accordingly, they must follow standard process to obtain credible results [9]. Similarly, the approach adopted in this investigation process has four phases [16]. By following this approach, it is possible to account for every data and evidence obtained during the examination. Besides, it easier to show time and hash values as proof of the investigation [14].

Evidence gathering from a storage media is backed with the fundamental steps in storage media investigation. They include extracting an image of the compromised system, performing hash value integrity calculation, recovery of files or folders to new locations, examining specific deleted files, and collection of evidence [17]. The evidence is collected from recycled folders, bad sectors, free spaces, auxiliary devices, network activity logs, and application software file. Also, gathering evidence involves proper copying of evidence into appropriate text files, relevant searches for key-term strings, and accurate scrutiny of applications or indication of file encryption, deletion, compression, and encryption or file hiding utilities. Therefore, the preparation of evidence summary should demonstrate, and report expert findings established from evidentiary excerpts and investigative examinations. The CIA (Confidentiality, Integrity,

and Availability) model is the fundamental security background for digital forensics investigation.

Conclusions

Digital forensic entails auditing in computer science that takes the evaluation, investigation, and analysis of computer systems to map digital assets and crimes. There is need to conduct a forensic investigation to unravel the damage caused, the extent of the attack, approach of the attacks and future measures to adopt in best practices and approaches in countering future cybercrime attacks. Technology and innovations have enabled in the development of new digital forensic tools with the ability to combine digital forensic investigations and digital forensic illegal activities. The research aimed at establishing the effectiveness of OSForensic in Digital Forensic Investigation to curb cybercrime. That is, the capabilities of OSForensics and the accuracy of OSForensics with regards to retrieving and analyzing data from a hard drive in order to investigate and curb cybercrime at the workplace. The research has established that OSForensics can effectively be adopted in forensic operations and with different capacities and capabilities. OSForensics tool enable the location of data while protecting the evidence and creating quality evidence to be used in legal proceedings. This tool is effective in curbing cybercrimes through determining and establishing criminal activities. OSForensics has analytical capabilities adopted in mining and analysis of criminal related data. Furthermore, the OSForensics tool enhances the digital investigation by use of Hash Set to establish safe files in operating systems or a program, thus making it possible to identify cybercrimes such as hacker scripts, viruses, or Trojans. OSForensic tool is vital in starting investigations since it has the capability of filling case details and creating new files. Additionally, the tool can mine data from recent downloads, access websites, and USB drives. OSForensics tool enhances the information security functions that enhance looking, mining, and reporting digital information for legal proceedings. The digital forensic tool is vital in identification, extraction, analysis, and presentation of digital evidence contained in digital devices. Like in the present case, OSForensics was able to identify company details that the suspected former employee was having. The research was able to identify sensitive information about the company that the suspected employee was having.

Acknowledgment:Big thank you for Umm A-Qura University for their support.

Ethical Clearance: Nil.

Source of Funding: Nil.

Conflict of Interest: Nil.

References

1. Hidayat A, Sudarmaji D, Irawan D, Susanto LJ, Mustika HP. Comparative Analysis Of Applications OSforensics, GetDataBack, Genius and Diskdigger On Digital Data Recovery in the Computer Device. International Journal of Engineering & Technology. 2018;7(4.7):445-8.
2. Kao DY, Chao YT, Tsai F, Huang CY. Digital evidence analytics applied in cybercrime investigations. In2018 IEEE Conference on Application, Information and Network Security (AINS) 2018 Nov 21 (pp. 111-116). IEEE.
3. Kebande VR, Ray I. A generic digital forensic investigation framework for internet of things (iot). In2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) 2016 Aug 22 (pp. 356-362). IEEE.
4. Kilungu MK. *An Investigation of Digital Forensic Models Applicable in the Public Sector (A case of Kenya National Audit Office)* (Doctoral dissertation).
5. Kishore N, Saxena S, Raina P. Big data as a challenge and opportunity in digital forensic investigation. In2017 2nd International Conference on Telecommunication and Networks (TEL-NET) 2017 Aug 10 (pp. 1-5). IEEE.
6. Lahaie C. Senator Patrick Leahy Center for Digitial Investigation.
7. Liakopoulou A. *Registration, classification and presentation of digital forensics and incident response tools* (Master's thesis, Πανεπιστήμιο Πειραιώς).
8. Losavio MM, Chow KP, Koltay A, James J. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy. 2018 May;1(3):e23.
9. Metivier B. Fundamental Objectives of Information Security: The CIA Triad [Internet].

Tylercybersecurity.com. 2021 [cited 26 February 2021]. Available from: https://www.tylercybersecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad

10. Naskar R, Malviya P, Chakraborty RS. Digital forensics: state-of-the-art and open problems. InBiometrics: Concepts, Methodologies, Tools, and Applications 2017 (pp. 1769-1787). IGI Global.
11. Nelson B, Phillips A, Steuart C. Guide to computer forensics and investigations. Cengage Learning; 2014 Nov 7.
12. OSForensics - FAQs - How much does OSForensics cost? [Internet]. Osforensics.com. 2021 [cited 26 February 2021]. Available from: https://www.osforensics.com/faqs-and-tutorials/how-much-will-osforensics-cost.html
13. OSForensics Pricing [Internet]. Osforensics.com. 2021 [cited 26 February 2021]. Available from: https://www.osforensics.com/pricing.html
14. Sansurooah K. A forensics overview and analysis of USB flash memory devices. InAustralian Digital Forensics Conference 2009 Mar 12 (p. 70).
15. Sabillon R, Serra-Ruiz J, Cavaller V, Cano JJ. Digital Forensic Analysis of Cybercrimes.
16. Sanap VK, Mane V. Comparative study and simulation of digital forensic tools. Int J Comput Appl. 2015;975:8887.
17. Sanchez L. *Multiplatformní HEX editor* (Bachelor's thesis, Českévysokéučenítechnické v Praze. Vypočetníainformační centrum.).
18. Wang X, Bai Y, Goda B. Project Design and Implementation for Digital Forensics Education. InProceedings of the 20th Annual SIG Conference on Information Technology Education 2019 Sep 26 (pp. 33-38).
19. Moyes E, Moyes E, Moyes E, Moyes E, Moyes E, Moyes E et al. Windows Bulletin Tutorials - [Internet]. Windows Bulletin Tutorials. 2021 [cited 26 February 2021]. Available from: http://windowsbulletin.com/
20. Place Orders / Request Quotes for New Licenses [Internet]. X-ways.net. 2021 [cited 26 February 2021]. Available from: http://www.x-ways.net/order.html