REVIEW

The application and effectiveness of Hex editor Forensic in investigating cybercrime

Bandr Siraj Fakiha, PhD

Abstract

Information Technology usage and development has improved the efficiency and the flexibility of service provision among a number of institutions. While the process of computerization is taking place at a very high speed, the security surrounding the critical asset of IT is a major growing concern for the top management. The application of the digital forensic concept can therefore be helpful in curbing problems associated with cybercrime. 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. Hex editor is one of the various digital forensic investigation tools that allow 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 paper seeks to establish the effectiveness of Hex editor in information technology security risk management. That is, the capabilities of Hex editor and the accuracy of Hex editor with regards to retrieving and analyzing data from a hard disc or drive in order to investigate and curb information technology security risk at the workplace. The researcher performed investigation on a Mozilla FxOS running on a phone released by Peak group in which case the researcher aimed to retrieve previous images that had been sent through the phone. In overall, Hex editor was able to identify the images and content of information that had been shared via the phone. Therefore, Hex editor is vital in identification, extraction, analysis, and presentation of digital evidence contained in digital devices. It is an effective tool that can be used by organizations for Forensic information technology security risk management. **Keywords:** Hex editor; Cybercrime; Digital Forensic; Investigation; technology, security, risk

Bandr Siraj Fakiha PhD
Umm Al-Qura University, Saudi Arabia
Email: bfageeha@hotmail.com

Received: July 06, 2022.
Accepted: December 15, 2022.
Conflict of interest: none.

Introduction

The development and usage of information technology has within the last decade improved the efficiency and flexibility in provision of services as most organizations currently depend on IT in performing most of their tasks. However, when the IT environment becomes more diverse and complex, it experiences numerous challenges in performing log management as well as real time response to incident and threat management [1]. Most common barriers to IT security are resources, awareness and cultural factors. Most organizations lack coordinated activities on IT security related issues such as Cyber safety. Similarly, there is oversight over IT security management in most organizations. In the event that such risks failed to be well taken care of, these organization objectives can be affected to a greater extent as well [3]. Moreover, most organizations lack appropriate technologies to investigate information security system breach.

In order to punish cybercrime, the organization leadership must establish some evidence. One of such evidence is the computers or digital device used by the suspect. The data stored in such a computer are taken as evidence in punishing perpetrators of cybercrime. Such evidence can only be obtained through what scholars refer to as forensic investigation [4]. The scope of the present project is therefore to establish the application and effectiveness of Hex

editor Forensic in information technology security risk management, specifically on matters of investigating cybercrime. Computer forensics refers to walking back through incidents in computer systems to investigate crimes or to map out digital assets [5]. Some of the types of digital forensics include computer forensics, firewall forensics, database forensics, and live systems forensics, and software forensics, etcetera. Of the said types, computer forensics is most essential as it involves analyzing and investigating for the collection and preservation of evidence.

Hex Editor, commonly referred to as HxD, is a tool that can perform the functions of opening and editing computer code. Furthermore [2] explains that Mael Horz developed HxD for Windows and that it edits the raw contents of disk drives, the application can also display and edit the memory getting used by running processes. According to [2], HxD supports the exportation of C#, C, Java, HTML, Visual Basic, disks, and disk images, etcetera. HxD can get integrated into the context menu for additional efficiency. Among the features of HxD is a RAM Editor that edits the main memory, a disk editor for RAW reading and writing of drives and disks, file comparisons, and the viewing of data in Ansi, DOS, EBCDIC and Macintosh character sets. In HxD, however, there is a fundamental statistical analysis of data. The proposed project sets to incorporate Hex Editor's analytical capabilities in the analysis of data obtained from data mining of criminal activities.

Materials and Methods

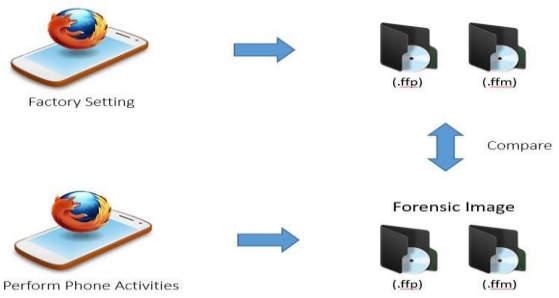
The research performed an investigation on Mozilla FxOS that was running on a phone that has been released by a phone called Peak. Having been introduced in the market back in 2013, the phone has a FxOS version. The specification of the phone is as shown below:

Figure 1 showing phone specifications

Hardware	Detail
Processor	1.2 GHz Qualcomm Snapdragon S4 8225 processor (ARMv7)
Memory	512 MB Ram
Storage	-Internal 4GB -Micro SD up to 16GB
Battery	- 1800 mAh - micro-USB charging
Data Inputs	Capacitive multi-touch IPS display

As shown in the above phone specification, the phone setting were initially wiped and subsequently restored back to the factory setting. The process of acquisition was then done to obtain FxOS phone image (.ffp) as well as the memory image (.ffm). These binary images were consequently marked as the base image and their respective MD5 hash values safely preserved. The investigator then installed social media application to the phone through the Mozilla Firefox. The investigator then simulated the real usage of the application by running a number of communication activities like uploading picture and sending private messages. All the steps, communication activities and credentials were appropriately documented in a manner that was forensically sound. A second acquisition process was then performed so as to identify and subsequently investigate the actual artefacts that would remain the type of credentials that could be extracted and the data that could be recovered after deleting. The illustration is shown in figure 2 below:

Figure 2 showing phone acquisition process



The evidence was then acquired through the use of Ubuntu 14.04 LTS and subsequently analysed in Windows10 machine. So as to capture the phone image in an appropriate manner using Ubuntu, the host phone was run under the Android Debug Bridge (ADB). The command below was applied to configure ADB package in the Ubuntu:
suto apt-got install android-tools-adb

For the purpose of volatile memory acquisition, the investigator configured Linux Memory Extractor (LiME) through the command below: # suto apt-got install-forensics-dkms

HxD Hex Editor 1.6.6.0 was subsequently installed in the machine to analyse the previously captured forensic images and messages that were

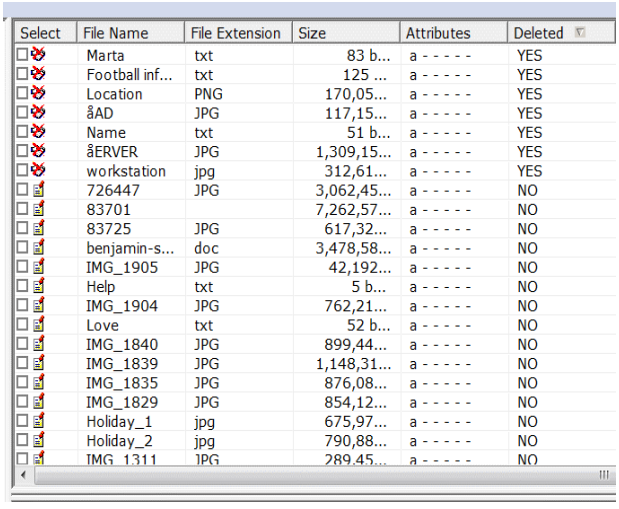
sent and received through the phone. Two types of the binary images that had initially been deleted were extracted, meant for use as forensic evidence in the investigation. More specifically, the binary image was extracted from the phone's internal memory by using the dd command. FxOS phone was initially connected to the specified host machine and then the ADB connection was initiated prior to executing the dd command. The following command was applied to begin ADB connection between the host machine and the phone: # adb shell

Once the connection had been established, the following dd command was performed to bit-by-bit copy the phone memory into the SD card and the file in this case was named as FxOS phone memory (.ffp):

dd if=/dev/block/mmcblk0 of=/mnt/emmc/base.ffp bs=2048

The entire binary image of the phone internal memory was subsequently copied from the SD card into the respective host machine and the file was named as ffp. 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

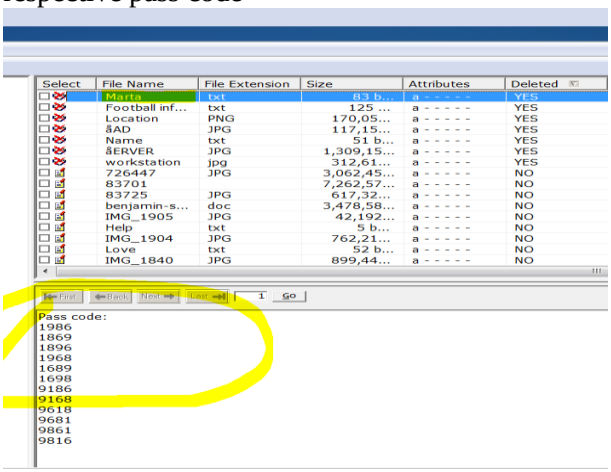
Figure 3 illustrating different folders extracted



Select	File Name	File Extension	Size	Attributes	Deleted
	Marta	txt	83 b...	a - - - - -	YES
	Football inf...	txt	125 ...	a - - - - -	YES
	Location	PNG	170,05...	a - - - - -	YES
	åAD	JPG	117,15...	a - - - - -	YES
	Name	txt	51 b...	a - - - - -	YES
	åERVER	JPG	1,309,15...	a - - - - -	YES
	workstation	jpg	312,61...	a - - - - -	YES
	726447	JPG	3,062,45...	a - - - - -	NO
	83701		7,262,57...	a - - - - -	NO
	83725	JPG	617,32...	a - - - - -	NO
	benjamin-s...	doc	3,478,58...	a - - - - -	NO
	IMG_1905	JPG	42,192...	a - - - - -	NO
	Help	txt	5 b...	a - - - - -	NO
	IMG_1904	JPG	762,21...	a - - - - -	NO
	Love	txt	52 b...	a - - - - -	NO
	IMG_1840	JPG	899,44...	a - - - - -	NO
	IMG_1839	JPG	1,148,31...	a - - - - -	NO
	IMG_1835	JPG	876,08...	a - - - - -	NO
	IMG_1829	JPG	854,12...	a - - - - -	NO
	Holiday_1	jpg	675,97...	a - - - - -	NO
	Holiday_2	jpg	790,88...	a - - - - -	NO
	IMG_1311	JPG	289,45...	a - - - - -	NO

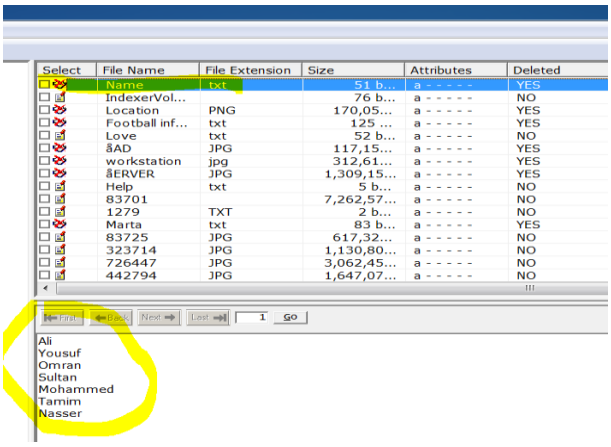
The investigation revealed some interesting files; for instance, Marta contained pass codes as shown in the figure below:

Figure 4 illustrating the file called Marta and respective pass code



The researcher also found another text file called "name" that had a list of people who had previously been communicated with:

Figure 5 illustrating the file called "name" with a list of suspected names communicated to



Results and Discussion

Hex editor 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 methodology, Hex editor 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, Hex editor was able to identify images and text information that had been shared through the phone. The research was able to identify sensitive information that could easily aid for further investigation in case there was a need. More specifically, the binary image was easily extracted from the phone's internal memory by using the dd command.

Such findings show that Hex editor can effectively be used for viewing and running of hexadecimal coded files. Hexadecimal file is for storing files that can be used. Hex editor can check the header and footer of the file format. For example, the JPG file format has specific header and footer FF D8 FF (header), FF D9 (footer). And for zip file format (ZIP) has also specific header and footer 50 4B 03 04 14 (header), 50 4B 05 06 00 (footer). Hex editor can find hidden data inside a file. For example, we can use Hex editor to find the hidden data by finding another header and footer different from the original header and footer.

As argued by [5], there are different researches and literature collection on digital forensic techniques and methodologies, such as the Windows environment. Digital forensic investigations entail the holding of devices and data contained. The data is gathered and compiled for investigation purposes. There are different digital forensic models adopted in the investigation and handling of forensic data such as investigative process model, forensic process, integrated digital investigation process, computer forensic. process, and computer forensic field triage process model [10]. The different models have four basic phases adopted in the investigation process. They include the preparation phase, the data acquisition phase, the investigation phase, and the reporting phase. The windows environment is comprised of different digital forensic tools such as HxD editor that enables mining of forensic evidence from implementing file indexing and searching as well as computers. In addition to that HxD Editor Tool is capable of file wiping, data recovery, cloning, and low-level disk imaging for purposes of forensic investigations. HxD Editor Forensic tool enhances securing disk wipes, recovery of deleted data, and supporting nondestructive disk analysis [9].

Regarding to [6] there are different digital forensic tools, the most common and effective tool is Hex editor. The tools are adopted in analysis and handling digital evidence that is prone to changes. Digital evidence can be transmitted and stored in different digital forms, thus needing specialized treatment using effective digital forensic tools. Hex editor tool is vital in starting investigations since it has the capability of filling case details and creating new files [5]. Additionally, the tool can mine data from recent downloads, access websites, and USB drives. Hex editor tool enhances the information security functions that enhance looking, mining, and reporting digital information for legal proceedings. It is vital in hiding hidden data inside different files for forensic investigations [8]. The digital forensic tool is vital in identification, extraction, analysis, and presentation of digital evidence contained in digital devices. Moreover [4] argue that there is a need to investigate the operation and effectiveness of different tools in identifying, gathering, and analysis of digital evidence for a legal proceeding. This approach enhances different organizations and individuals to determine the tools that suit their operations and type of work.[9]

Highlights that even in the event that the suspect had deleted all files and overwritten them from the hard disk, one can easily apply a hex editor to retrieve any data that had previously been stored both within the disk sectors and the files. A hex editor specifically makes it possible for one to peek at the individual physical contents that are stored within the disk, irrespective of the file boundaries, partitions and directories. As claimed by [5], Hex editors can easily be applied to crack even copy-protected software, study the manner in which viruses in computer work, or in the process of forensic investigation, identify and subsequently retrieve specific information that cannot be accessed normally by the operating system.

One need to understand that all information saved within the hard disk are always recorded within the tracks, which are actually concentric rings within the surface of each individual hard disk platter, such as the rings within a tree trunk [7]. Hex editors have the ability to directly read the physical medium buffer without having to depend on the services of any operating system.

Conclusion

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 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 technologies existing in digital forensic investigations, measures to improve digital forensic investigations, and challenges experienced in the course of using digital forensic. The research has established that HEX Editor can be adopted in forensic operations and with different capacities and capabilities. HEX Editor Forensic tools 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. Hex Editor has analytical capabilities adopted in mining and analysis of criminal related data. Furthermore, the 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. Hex Editor Incident response allows the investigation of the digital information without alerting valuable metadata such as last time accessed. Therefore, the Hex Editor tool can be applied by the organization as it enhances the information security functions that enhance looking, mining, and reporting digital information for legal proceedings. The digital forensic tool in this case can be vital in the identification, extraction, analysis, and presentation of digital evidence contained in digital devices.

Acknowledgment: As usual special and big thank you for Umm Al-Qura University.

References

1. Hsu, Y.M. and Chang, C.C., 2011. Analysis and improvement on frequency sensitivity of series photodetector frequency circuit system and its application for HEX fluorescence measurement. Optical Engineering, 50(4), p.044401.
2. Schaefer, T., Höfken, H. and Schuba, M., 2011, October. Windows phone 7 from a digital forensics' perspective. In International Conference on Digital Forensics and Cyber Crime (pp. 62-76). Springer, Berlin, Heidelberg.
3. Simon, M. and Slay, J., 2010, February. Recovery of skype application activity data from physical memory. In 2010 International Conference on Availability, Reliability and Security (pp. 283-288). IEEE.
4. Blakeley, B., Cooney, C., Dehghantanha, A. and Aspin, R., 2015, November. Cloud storage forensic: hubiC as a case-study. In 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 536-541). IEEE.
5. LeMaster, A., 2011. Heap spray detection with heap inspector. Blackhat USA, Las Vegas, Nevada, US.
6. Naick, B.D. and Bachalla, N., 2016. Application of Digital Forensics in Digital Libraries. International Journal of Library & Information Science (IJLIS), 5(2), pp.89-94.
7. Jain, N. and Kalbande, D.R., 2015, September. Computer forensic tool using history and feedback approach. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-5). IEEE.
8. Ryczkowski, A. and Piotrowski, T., 2011. Tomotherapy archive structure and new software tool for loading and advanced analysis of data contained in it. Reports of Practical Oncology & Radiotherapy, 16(2), pp.58-64.
9. Sanchez, L. (2017). Multiplatformní HEX editor (Bachelor's thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum.).
10. Sun, J.L., Zhang, S.W., Huang, S. and Hui, Z.W., 2018, July. Design and application of a Sikuli based capture-replay tool. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 42-44). IEEE.