REVIEW

Cybersecurity: Analysis and Application of ProDiscover Forensic Toolkit

Bandr Siraj Fakiha PhD

Abstract

The world has in the recent past experienced rapid development in digital technology. However, as most organizations across the world continue to introduce digital technology into their operating system, issues of cybercrime have been on the rise and are one of the major threats to the progress and growth of many business firms. The application of the digital forensic concept can therefore be helpful in curbing problems associated with cybercrime. ProDiscover is one of the forensic tools which enable professionals in computing to locate all data in computing disk, including those that had previously been deleted. ProDiscover Forensic tool recovers deleted files, examines slack space, and dynamically allows previews, image captures, and searches of the Hardware Protected Area (HPA) using its technology. This paper sought to establish the application and effectiveness of ProDiscover Forensic in investigating cybercrime. For the purposes of this paper, efficiency will be defined as the proportion of input required by the ProDiscover system compared to its performance and output in addressing and managing workplace cybercrime. Alternatively, effectiveness will be defined as the degree and capacity to which the system will succeed in improving forensic investigation and mitigating cybersecurity issues in the workplace. That is, the capabilities of ProDiscover Forensic with regards to investigating and punishing cybercrime offence at the workplace. The researcher investigated a case in which a company by the name Jonson Corp. had been complaining about one of their staff, a Mr John who had been using the computer system for viewing and subsequently downloading pornographic images. The suspect's floppy disk of 1.44 MB capacity that had been found in his drawer was used to retrieve all the deleted files. In overall, ProDiscover was able to retrieve the BEAUTY1.jpg and BEAUTY2.jpg images that had been erased from the soft disk. Therefore, the ProDiscover tool can be applied by organizations to enhance their information security functions, especially during a forensic investigation.**Keywords—**Cybercrime, ProDiscover, Forensic investigation, Digital forensic, Cybersecurity

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

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

Introduction

Despite the numerous benefits associated with Information Technology, various business organizations are facing a major threat known as cybersecurity. Incidences of system hacking and intrusion by cybercriminals are proving to be so high. According to a Forbes news article by Brooks (2022), approximately 93% of all company networks are vulnerable to cybercriminal intrusion. The article also reports that the research and educational sector is most targeted by these criminals, followed by the health care, ISP and MSP, and communications sectors. Further, ransomware as a cybersecurity issue incurred over $20 billion globally in 2021 and affected about 37% of all enterprises and business organizations (Brooks, 2020). Protection from the cybersecurity issue has cost the world approximately $1 trillion from 2017-2021, which is expected to rise to $1.75 trillion over the next five years (Brooks, 2020). The problem of cybercrime can adversely affect the individual users of such system, small and large business organizations in addition to some important financial implications, for example, direct costs like stealing of money, digital assets and sensitive information. It can also cause a number of indirect costs with regards to service interruption, low level of productivity and general legal liability that is experienced due to diverted resource like computer power, capital and bandwidth which can further lead to a number of costs that are associated to the long-term effects on an attack on the brand image, bad reputation and competitiveness (Budzier, 2011). In order to punish cybercrime, the organization leadership must establish some evidence. One of such evidence is the computers 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. Computer forensics refers to walking back through incidents in computer systems to investigate crimes or to map out digital assets. 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 (Naskar et al., 2017).

Literature Review

Cybersecurity threats

Literature has affirmed that Information communication in the current times has become more effective and efficient (James, Nottingham & Kim, 2013). Even with that, however, security concerns over having the safe transfer of data has been on the rise. Cyber-attacks as well as some other related threats that are targeted at the system of information communication are rendering network and system security becomes an aspect worth giving deeper consideration within the realm of information communication technology (Kim, et al., 2015). With the advance in technology, hackers and intruders have within their own disposal very complicated tools which they can use to bypass the traditionally known generic network security system to cause intended harm in the whole system (James, Nottingham & Kim, 2013). Specifically, cybersecurity threats are currently exploiting the connectivity and complexity found in the existing infrastructure and launch attacks on systems considered as legitimate. Even with such predicaments, it is important to note that the economic performance of any company usually depends on the reliable working of the important infrastructure, whose safety might be put at a higher risk by the cyber-attacks (James, Nottingham & Kim, 2013).Such kind of attacks has major impacts on the general financial viability of the organization that might have been affected and even on the general reputation of the company (James, Nottingham & Kim, 2013). System failures and crashes are good examples of the risks that most organizations dread currently in their day-to-day operations and for which numerous security measures have been considered necessary.

Flores, Qazi & Jhumka (2016) acknowledges that cyber-security threats have continued to evolve, a rise, and subsequently take a new form. Symantec (2016) records that 430 million new malware pieces were detected in 2015, representing a 36% increase from what had been recorded in 2014. With the rising rate at which small businesses continue to adopt technology, these statistics leave them highly vulnerable.

Despite the challenges associated with cybersecurity, small business companies are continually going through a radical transformation for the need for embracing the current age of information (Azodolmolky, Wieder & Yahyapour, 2017). This has always ended up making them rely on information technology for the need to handle some important part of their main service deliveries and, consequently, a proper asset that is very valuable for the information of the whole organization. Protection against the risk associated with cybersecurity is one of the most important things that current business organizations need to look up to. Bandyopadhyay, Jacob & Raghunathan (2010) claims that while many organizations are moving forward towards creating E-service and making their information more digital, convenient, and accessible, there is a great risk that comes with it, a severe cyber threat. The data is likely to be stolen, hacked, wiped, or even sabotaged.

Among such measures has always been the detection system for any form of network intrusion (Wang, Chao & Wang, 2015). Network Intrusion Detection System usually analyzes and predicts behaviours of a given system with the main aim of countering such activities that it might interpret as suspicious (James, Nottingham & Kim, 2017). The intrusion, in this case, can always occur in varied ways, a legitimate user of a given system misusing the privileges they have of accessing the system, a legitimate user trying to gain additional access privileges, and lastly, an external attacker trying to access the system (James, Nottingham & Kim, 2013). The network intrusion detection system in this case works by either recognizing the attacks or malicious activities or blocking them or detect by looking at the signatures of the attack within the log files. Even with such a security system, however, organizations are yet to achieve much with the current network security systems (Farahmand, et al., 2005). In order for any business organization to be safe from cyber threats, they require a complex security system that can protect the existing computer networks from dangerous threats. The security system can comprise of firewalls, a system that detects and prevent intrusion and solutions for path management, together with some strong anti-virus.

Application of ProDiscover Forensic in investigating cybercrime

ProDiscover Forensic is a computer forensic tool which "7 Best Computer Forensic Tools" (2019) describes as powerful that enables professionals in computing to locate all data in computing disks, including those that had previously been deleted. ProDiscover Forensic tool recovers deleted files, examines slack space, and dynamically allows previews, image captures, and searches of the Hardware Protected Area (HPA) using its technology ("7 Best Computer Forensic Tools," 2019). While "7 Best Computer Forensic Tools" (2019) describes the power of the ProDiscover Forensic tool, this tool does not determine cyber-attack patterns and find motives for cyber-attacks as the system for this project will. The forensic and concepts used in ProDiscover Forensic, however, will be useful to the project since the project reQquires digital forensics in assisting to curb the issue of cybercrime through determining criminal activities.

Some of the features of this software include recovery of deleted data, secured disk wipe, and the support of non-destructive disk analysis. According to Sanap and Mane (2015), the software's s full Boolean search capability implies it can explore the entire disk for phrases, keywords, and regular expressions. Besides, its hash compatibility permits the isolation of illegitimate files from the good system files.

The ProDiscover Forensic 4.9 Toolkit costs approximately $ 2,195 (Windowsbulletin, 2019). However, the one-time purchase allows a single forensic investigation of the entire system (SC Media, 2008). The tool offers an in-built reporting tool for presenting shreds of evidence in case of legal proceedings. Additionally, it collects time zone information, internet activities, and drive information. Therefore, the software has a comprehensive search capability for obtaining unique file and data names, data patterns, file types, and date ranges.

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 (Kilungu, 2015). 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 OSForensics, HxD editor, and ProDiscover. OSForesnic enables mining of forensic evidence from implementing file indexing and searching as well as computers. HxD Editor Tool is capable of file wiping, data recovery, cloning, and low-level disk imaging for purposes of forensic investigations. ProDiscover Forensic tool that enhances securing disk wipes recovery of deleted data, and supporting non-destructive disk analysis (Dweikat, Eleyan & Eleyan, 2020).

Methodology

The paper explores the ProDiscover Forensic Toolkit in the context of workplace cybersecurity surveillance, management, and control. It introduces the issue and provides a credible, relevant, and reliable to improve the quality and quantity of related content. Then, it explores a case of the Jonson Corp, where an employee has been accused of cybersecurity violations, and illustrates the efficiency and effectiveness of the Prodiscover Forensic Toolkit in conducting the investigation.

The paper attempts to document a personal research investigation on a staff member, Mr. John, at Jonson Corp. It starts by placing the cybersecurity issue into context using evidence from various reliable sources and illustrates how and why corporations should formulate strategies to enhance protection against current and future threats. The paper details how the ProDiscover Forensic Toolkit was applied to investigate allegations against the employee, which entailed complaints about his unethical use of the company's computer. Hence, using findings from the paper, organizations, business enterprises, and other researchers may improve their awareness of possible cybersecurity enhancement tools and techniques, such as the ProDiscover Forensic Toolkit, and enhance overall workplace safety and security.

The information entailed in the paper was collected based on criteria of credibility, relevance, and date. All sources were peer-reviewed, academic and scholarly, and retrieved from credible technology-related bodies such as Information Technology and Management and the IEEE Communications. Additionally, the sources had to be related to the cybersecurity topic and explore aspects such as networking, forensics, forensic tools, and data retrieval. These sources were also no more than 18 years old to ensure the information was relatively recent, because the body of knowledge of cybersecurity, as an aspect of technology and the Internet of Things, is expanding and advancing exponentially.

The paper has no conflicts of interests. As most information was retrieved online, financial constraints did not arise from the research process. Additionally, the paper was awarded ample time for completion. Hence, time constraints did not limit the planning, formulation, and completion of the paper. The lack of these constraints resulted in unaffected findings and conclusions, contributing to the reliability and credibility of the paper.

Results and Discussion

Digital forensic investigators follow the specific stages and measures when working on an incidence. For that reason, the investigator is likened to tools because they act as tools in tracking and persecuting criminals. Accordingly, they must follow a standard process to obtain credible results. Similarly, the approach adopted in this investigation process had four phases as proposed by Kilungu (2015). 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.

The researcher investigated a case in which a company by the name Jonson Corp. had been complaining about one of their staff, a Mr John who had been misusing their computer system. The company had a doubt that he had been using the computer system for viewing and subsequently downloading pornographic images. The company was looking for evidence to implicate the suspect in question. During the search of physical material from the suspect's drawer, a floppy disk was found of 1.44 MB capacity. The Floppy disk was labelled John.

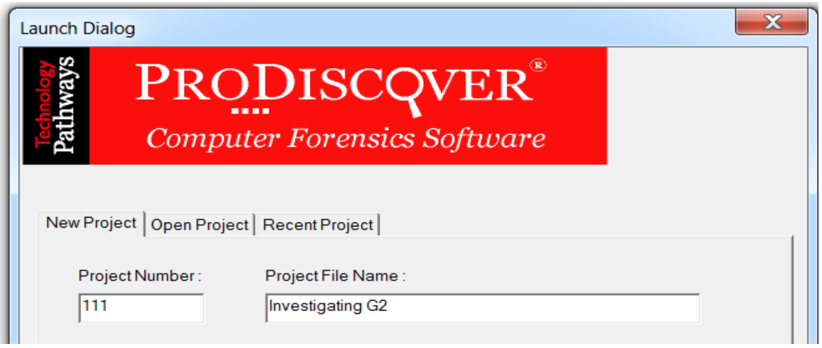
According to Lovanshi & Bansal (2019), evidence gathering from storage media like the case of John's floppy disk was backed with the fundamental steps in storage media investigation. They included extracting an image of the compromised system, performing hash value integrity calculation, recovery of files or folders to new locations, examining specific deleted files, and collection of evidence. The evidence was collected from recycled folders, bad sectors, free spaces, auxiliary devices, network activity logs, and application software file.Also, gathering evidence involved 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.

To examine the violation by John, the investigators decided to use the four-phase process. The first step was the investigation phase, which involved seeking permission from the relevant authority to search and seiZe the materials. The scene was secured, and the chain of custody of items seized was documented. Notably, the investigator prioritized the actions and justified the resources for the investigation.

The data acquisition phase involved obtaining digital evidence by first launching ProDiscover Forensic 4.9 software as shown in the figure below:

The tool (ProDiscover Forensic 4.9) was used to create a computer forensic image of the confiscated evidence. Before image creation, the MD5 hash value of the digital evidence, floppy disk, was calculated for authenticity. Subsequently, the forensic image of the evidence was examined in the investigation phase. More specifically, we clicked on the image to view its.

Figure 1: ProDiscover Forensic Software Configuration

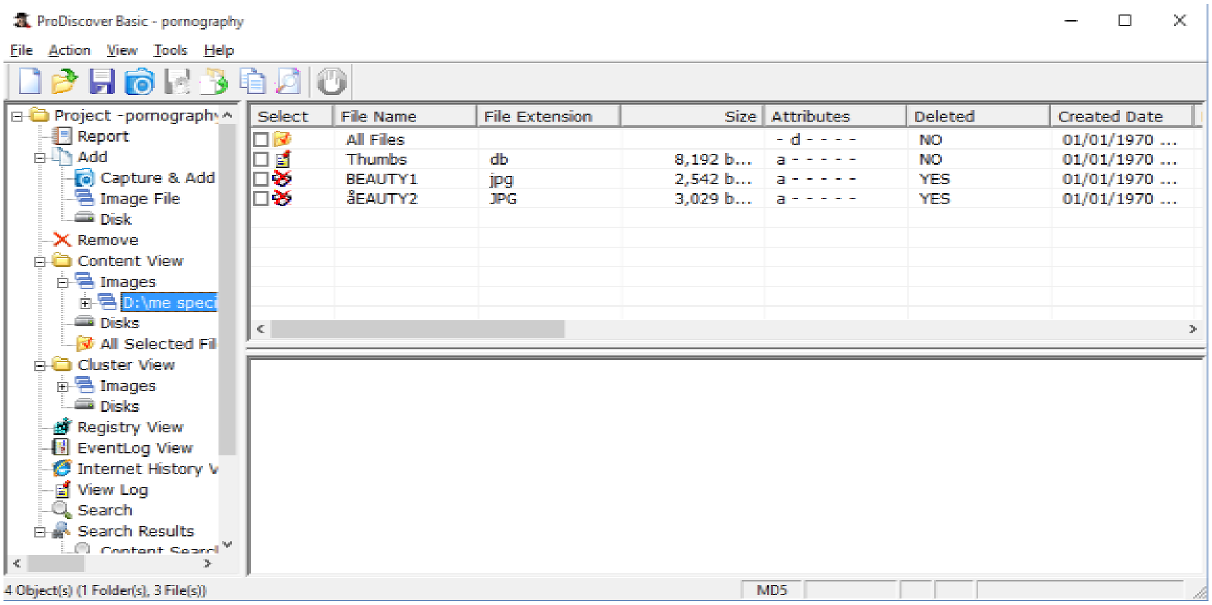


Project Number : 111

Project File Name : Investigating G2

Source: Created by author using ProDiscover Forensic Toolkit

Figure 2: Recovered Files Using ProDiscover Forensic



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date
□	All Files			- d - - - -	NO	01/01/1970 ...
□	Thumbs	db	8,192 b...	a - - - - - -	NO	01/01/1970 ...
□	BEAUTY1	jpg	2,542 b...	a - - - - - -	YES	01/01/1970 ...
□	åEAUTY2	JPG	3,029 b...	a - - - - - -	YES	01/01/1970 ...

4 Object(s) (1 Folder(s), 3 File(s))

Source: Created by author using ProDiscover Forensic Toolkit

content. This made it possible to see the content of the disk image within the right pane. As shown in the figure below, the investigators were able to view the BEAUTY1.jpg and BEAUTY2.jpg images that had been erased from the soft disk

ProDiscover Forensic 4.0 software offered hard disk security examination. The software was able to give detail on what had been deleted from the floppy hard disk. Once it was launched and a forensic image of the confiscated evidence created, ProDiscover Forensic automatically generated a report together with the much-needed information to be submitted as evidence for legal action.The software helped in gathering the time zone data, internet activity, and drive information. In the long run, the investigators were able to view BEAUTY1.jpg and BEAUTY2.jpg images that had been erased from the soft disk

These results confirm the findings by Sanap and Mane (2015) who carried out a study using the outlined phases using the ProDiscover software to analyze a bootable' file. Based on the simulated results of a comparative study, ProDiscover works best in data recovery. The basis for comparison of Active File Recovery, ProDiscover was based on the following aspects: supported file system, file investigation, log investigation, index of deleted file, supported disk images, and memory dump investigation (Conner, 2020). Since the ProDiscover tool exhibited unique advantages, the merit for selection depended on the requirements and applications of the tool.

According to Hidayat et. al. (2018), ProDiscover software restores deleted data effectively, particularly data removed by the perpetrators. In their study, Sharma & Nagpal (2020) carried out a four-phase comparative analysis of ProDiscover. They made the comparison with Disk Genius, GetDataBack and Diskdigger forensic toolkits for data retrieval on Windows 8 Operating System (Ghazinour, et al., 2017). Analysis began with formatting the floppy disk drive and then filling out data on the disk drive.All the data in the disk was deleted and the recycle bin emptied. The digital forensic toolkits were then used for data recovery. The ProDiscover kit recovered the deleted data precisely compared to Disk Genius, GetDataBack and Diskdigger (Hidayat, Sudarmaji, Dedi, & Lilik, 2018).

Conclusion

ProDiscover forensic is a very useful tool as it offers powerful information security functionalities. This tool can effectively be applied by digital forensic experts to look for digital information for use in reports for legal proceedings. ProDiscover allows for keyword searches.For example, in the investigation shown above, the researcher was able to identify the already deleted file, their contents and names. Additionally, one can search deleted files, by modified date, accessed date and created date for the files. ProDiscover Incident response allows the investigation of the digital information without alerting valuable metadata such as last time accessed. Therefore, the Pro discover 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. 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 the organization’s capabilities to investigate and adequately respond to cybercrime.

References

7 Best Computer Forensic Tools. (2019, February 18). Retrieved from https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref

Azodolmolky, S., Wieder, P., & Yahyapour, R. (2017). Cloud computing networking: challenges and opportunities for innovations. *IEEE Communications Magazine*, *51*(7), 54-62.

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology And Management*, *11*(1), 7-23. doi:10.1007/s10799-010-0066-1

Brooks, C. (2022, January 21). *Cybersecurity in 2022 – A fresh look at some very alarming stats*. Forbes. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

Budzier, A. (2011). The risk of risk registers – managing risk is managing discourse not tools. *J Inf Technol*, *26*(4), 274-276. doi:10.1057/jit.2011.13

Conner, T. (2020). *A Review of the Challenges Anti-Forensics Present to the Viability of File Recovery* (Doctoral dissertation, Utica College).

Dweikat, M., Eleyan, D., & Eleyan, A.(2020). Digital Forensic Tools Used in Analyzing Cybercrime.

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology And Management*, *6*(2-3), 203-225. doi:10.1007/s10799-005-5880-5

Flores, D. A., Qazi, F., & Jhumka, A. (2016, August). *Bring your disclosure: analysing BYOD threats to corporate information*. Paper presented at 2016 IEEE International Conference on Turst, Security and Privacy in Computing and Communications, Tianjin, China.

Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. In *2017 IEEE international conference on power, control,* *signals and instrumentation engineering (ICPCSI)* (pp. 3136-3142). IEEE.

Hidayat, A., Sudarmaji, D., Irawan, D., Susanto, L. J., & Mustika, H. P. (2018). Comparative Analysis Of Applications OSforensics, GetDataBack, Genius, and Diskdigger On Digital Data Recovery in the Computer Device. International Journal of Technology & Engineering, 7(4.7), 445-448.

James, T., Nottingham, Q., & Kim, B. (2017). Determining the antecedents of digital security practices in the general public dimension. *Information Technology And Management*, *14*(2), 69-89. doi:10.1007/s10799-012-0147-4

Kilungu, M. K. (2015). An Investigation of Digital Forensic Models Applicable in the Public Sector: A case of Kenya National Audit Office. Nairobi: University of Nairobi.

Kim, S., Kim, G., & French, A. (2015). Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. *Information Technology And Management*. doi:10.1007/s10799-015-0217-5

Lovanshi, M., & Bansal, P. (2019). Comparative study of digital forensic tools. In *Data, Engineering and Applications* (pp. 195-204). Springer, Singapore.

Naskar, R., Malviya, P., & Chakraborty, R. S. (2017). Digital Forensics

Sanap, V. K., & Mane, V. (2015). Comparative Study and Simulation of Digital Forensic Tools Tools. International Conference on Advances in Science and Technology (pp. 1-4). Mumbai: Ramrao Adik Institute of Technology.

SC Media. (2008, May 7). *Security Weekly Labs: Technology Pathways ProDiscover Forensics 4.9*. https://www.scmagazine.com/editorial/product-test/-/technology-pathways-prodiscover-forensics-4-9

Sharma, P., & Nagpal, B. (2020). Regex: an experimental approach for searching in cyber forensic. *International Journal of Information Technology*, *12*(2), 339-343.

Symantec. (2016). Internet security threat report (21). Retrieved from https://know.elq.symantec.com/e/f2

Wang, P., Chao, K., Lo, C., & Wang, Y. (2015). Using ontologies to perform threat analysis and develop defensive strategies for mobile security. *Information Technology And Management*. doi:10.1007/s10799-014-0213-1

Windowsbulletin.com. (2019). ProDiscover Basic and ZeroView. Retrieved February 14, 2020, from Windows Bulletin-Tutorials: http://windowsbulletin.com/de/files/exe/technology-pathways/prodiscover-basic-and-zeroview/