Print ISSN: 2233-4165 / Online ISSN 2233-5382
JIDB website: http://www.jidb.or.kr
doi:http://dx.doi.org/10.13106/jidb.2021.vol12.no6.47

Digital Forensic: Challenges and Solution in the Protection of Corporate Crime

Do-Hee CHOI[1]

eceived: April 14, 2021. Revised: May 22, 2021. Accepted: June 05, 2021.

Abstract

Purpose: Organizational crime is an offense committed by an individual or an official in a corporate entity for organizational gain. This study aims to explore the literature on challenges facing digital forensics and further discuss possible solutions to such challenges as far as the protection of corporate crime is concerned. **Research design, data and methodology:** Qualitative textual methodology matches the interpretative approach since it is a quality method meant to consider the inductivity of strategies. Also, a qualitative approach is vital because it is distinct from the techniques used in optimistic paradigms linked to science laws. **Results:** For achieving justice through the investigation of digital forensic, there is a need to eradicate corporate crimes. This study suggests several solutions to reduce corporate crime such as 'Solving a problem to Anti-forensic Techniques', 'Cloud computing technique', and 'Legal Framework' etc. **Conclusion:** As corporate crime increases in rate, the data collected by digital forensics increases. The challenge of analyzing chunks of data requires digital forensic experts, who need tools to analyze them. Research findings shows that a change of the operating system and digital evidence interpretation is becoming a challenge as the new computer application software is not compatible with older software's structure.

Keywords: Digital Forensic, Corporate Crime, Theoretical Literature Analysis

JEL Classification Codes : G30, D83, C35

1. Introduction

What exactly does the concept of digital forensic entail? And how does it relate to corporate crime? Developing curiosity in understanding these two concepts is vital in understanding, acknowledging, and appreciating the importance of digital forensic in a world where incidences of corporate crime continue to increase daily due to challenges of investigation. Digital forensic, also called digital forensic science, emanates from the main branch of forensic science. Forensic science involves examining and analyzing pieces of evidence from a crime scene or any other place that a crime may be suspected to have occurred. The primary objective is to establish an objective investigation that helps prosecute criminals involved in the crime. Depending on the findings' objective, the investigation can also be used to absolve an innocent individual who may be suspected to be a criminal. Therefore, as a branch of forensic science, the concept of digital forensic also focuses on recovering and investigating criminal incidences and materials existing in digital devices, often involving computer crime.

On the other hand, corporate crime or an organizational crime is an offense committed by an individual or an official in a corporate entity for organizational gain. Often, such officials rarely view themselves as criminals or rather the activities they engage in such as criminal activities. White-collar crimes are often characterized by their ability to not being visible. They are rarely easy to be detected because they are often conducted so that no individual can

1 First Author and Corresponding Author, Graduate student of Forensics, Sungkyunkwan University, Seoul, Korea,
Email: dkrlsla1@daum.net

tell the form of action or channel of communication as they always ensure they maintain the legal framework. These aspects make it difficult to detect a corporate crime. They are also characterized by the distance aspect often between the incident of the offender and the victim. The offender will often appear to be far from the victim, and as such, they will appear to be innocent. Corporate crimes may entail bribery among public officials, embezzlement of public funds, stock market manipulation, environmental damage resulting from negligence, among many others. The effects of corporate crimes may be social or economic. The mind of an individual, their body, and the environment may be affected. Often victims are witnessed to have bitterness, depression, health issues, and even anger. Economically, it damages economic stability by eliminating the trust of investors.

Corporate crimes have not been easy to control as most of those involved are elite members of the society who equally highly educated. This aspect has made corporate crime to be a high threat than local crimes performed on streets as such is easy to manage. Society continues to be affected negatively by corporate crimes. As the economy witnesses an increase in companies' privatization, cases of corporate crimes also continue to increase (Nantharath, Laochankham, Kamnuasilpa & Kang, 2020). However, with advancements in technology, digital forensic has significantly impacted most corporate crimes, bringing the perpetrators to record. Civil cases in courts of law continue to hold individuals accountable for what they did. Even though various challenges are witnessed in digital forensic, solutions to addressing such challenges also continue to be witnessed as technology advances. The challenges often witnessed are technical, regal, and resource challenges. It becomes easy to manage and control the increasing rate of corporate crimes in the World by addressing these challenges. Therefore, this paper will be exploring the literature on challenges facing digital forensics and further discuss possible solutions to such challenges as far as the protection of corporate crime is concerned.

2. Literature Review

The digital forensics has witnessed significant progress since its first application by Hans Gross between 1847 and 1915 to conduct a scientific criminal investigation (Zubańska, 2018). This marked the first impact of digital forensic, which was by then called computer forensic. Later in 1932, the Federal Bureau of Investigation in the United States of America considered establishing a laboratory that would provide forensic services to law authorities in the United States of America and other field agents related to security and law enforcement. This effort contributed to shedding more light on the need and importance of integrating computer forensic in security firms. In 1978, Florida became the first to pass the computer crime Act to strengthen the law enforcement system (Li, 2017). It also enhanced the development of digital forensic.

This development was equally significant progress in embracing digital forensic in the criminal investigation. Francis Galton is also recognized to have contributed to the development of digital forensic between 1982 and 1911. His effort witnessed the introduction of the first fingerprint, which is also an essential element in forensic investigation. The use of fingerprints continues to be used even today in helping the government to conduct investigations. The evolution witnessed the first use of computer forensic in academic studies. The progress also enhances another step-in computer forensic development through the formation of the International Organization on Computer Evidence (IOCE) in 1995. It was in 2010 when Simson considered addressing challenges facing digital forensic (Vincze, 2016). Most of these challenges have been witnessed to protect corporate crimes.

Forensic science challenges can be categorized into technical challenges, legal challenges, and resource Challenges (Vincze, 2016). Technical challenges are related to the advancement in technology. This article's findings show that the more technology develops, corporate crimes and criminal activities also continue to be witnessed in organizations. Most of these criminals witness the changes that are embraced in digital forensic, and as such, they also develop strategies on how to carry out their criminal activities. This poses a challenge to the digital forensic team responsible for carrying out investigations to uncover such criminal activities. Experts working in digital forensic departments often use various instruments and technologies to gather evidence in data related to corporate crimes. However, criminals also apply the same tools to hide, changing or eliminating traces of the crime they have conducted in organizations. This challenge is often referred to as an anti-forensic technique, and it has remained a primary challenge in the digital forensic effort (Park, Park, Kim, Cheon & James, 2017). Corporate criminals are also trying to ensure that they also advance their tricks in covering the crimes as technology advances.

Various anti-forensics techniques are often used; encryption, data hiding storage space, and covert channel (Wani, Wani, AlZahrani & Bhat, 2020). Encryption is legally used to secure information to achieve privacy by hiding it from those not authorized to access it. However, criminals have also managed to use it in hiding pieces of evidence relating to their crimes. Also, studies show that criminals in organizations often use a large amount of data within the storage medium so that such data cannot be

visible. They achieve this effort by applying system commands, among other programs (Kumar et al., 2019). This aspect poses a challenge to the digital forensic department as they cannot uncover evidence of corporate crimes in organizations. Criminals end up getting used to committing corporate crimes as they know they will not be held accountable because there is no evidence. According to Elsadig and Fadlalla (2016), the covert channel is also a challenge facing the digital forensic in modern technology. The concept refers to a communication protocol that enables a criminal to evade interference detection techniques to hide essential data on the network. This technique is often used by criminals to hide their crimes in organizations.

Operating in the cloud is another technical challenge as the digital forensic departments try to address corporate crimes in organizations. Operating in the cloud refers to the centralization of a company's data system. However, criminals have not been left in darkness about this advancement in digital forensic. Criminals are now aiming at cloud providers to access the cloud system data. This aspect makes the digital forensic department rethink how to address the issues so that operating in the cloud remains safe and reliable for preventing criminals from hiding and interfering with the evidence of crimes.

Studies have also shown that digital forensics is also facing legal challenges that continuously affect uncovering corporate crimes in organizations. According to Omolaye-Ajileye (2016), presenting digital forensic evidence is facing difficulty, making even the collection of data easier than the judicial system's presentation. The existing legal framework does not acknowledge the effort by the digital forensic sector in uncovering corporate crimes. For instance, studies have cited an example of the Jagdeo Singh V. The State and Ors (Omolaye-Ajileye, 2016). The legal framework in this case scenario shows how the court undermines the effort of digital forensics. I the case scenario above, the admissibility aspect of an intercepted phone call that had no certificate was not considered by the court as an evidence, and as such, it was dismissed hence leaving the corporate crime uncovered (Omolaye-Ajileye, 2016). Apart from this case scenario that happened in India, electronic evidence has often challenged courts of law due to the integrity issue. The court claims the evidence presented by digital forensics lack integrity and as such, they cannot be used as sources of evidence to seek justice against corporate crimes. Lack of a proper framework and guidelines, and explanations in gathering information, pauses a challenge to digital forensic forensics.

India as an example of a country whereby there is no legal framework to help guide the digital forensic department in collecting data or electronic evidence aimed at eliminating corporate crimes. Due to this challenge, digital forensics in countries like India have opted to with their own guidelines in collecting electronic data to provide evidence. The legal evidence Act in India has also remained without embracing change as time goes by. It, therefore, limits the digital evidence and its applicability. This aspect becomes difficult for the investigation to uncover evidence of corporate crimes. Other legal challenges affecting digital forensics entail privacy issues, analysis of a running computer, digital evidence storage, and the framework for collecting digital evidence.

Table 1: Summary of the Present Research Findings

Challenges	Summary
Technical Issues	-The Encryption software that digital forensic have been using have also contributed to the challenge of accessibility of crimes evidence by criminals hence contributing to the deletion or other forms of data interference. -•Operating in the cloud; Criminals arenow aiming at cloud providers to access the data in the cloud system.
Legal Issues	-Lack of legal framework and guidelines; Hinders the presentation and evidence in courts of law. -Limitations by Acts of law; Some Acts of law have undermined the effort of the Digital forensic
Resource Issues	-Change in technology; has affected the integration of old software and the new software hence leading to loss of data -High volume of data: As the amount of data increases, analyzing the data becomes a challenge.

Studies have also cited resource challenges in digital forensics. As corporate crime increases in rate, that data collected by digital forensics also increases (Årnes, 2017). The challenge of analyzing such chunks of data requires digital forensic experts who need various tools to analyze the data. Since the forensic data is highly sensitive, it requires a high-security level while using the tools to authenticate the data (Warren, El-Sheikh & Le-Khac, 2018). However, keeping these tools secured from intruders is also a challenge as most criminals have managed to access them to alter or interfere with the data evidence. This aspect of altering the data undermines the effort of digital forensic experts in uncovering corporate crimes. Additionally, research shows that a change in technology such as the operating system, computer application software and hardware, and digital evidence interpretation is becoming a challenge as the new computer application software is not compatible with the data

structure in older software. Further, the volume data is also one of the challenges that studies have shown hinder digital forensics. According to Harshany, Benton, Bourrie and Glisson (2020), the larger the volume of data handled by digital forensics, the higher the vulnerability of the data to unauthorized users.

3. Research Design

An analysis from the previous study revealed that an interpreter excludes natural science (quantitative) methodologies since a qualitative methodology adopts a knowledge of individuals' reality. There is no unique reality because there are different definitions of leadership in the interpretative model (Woo & Kang, 2020). As a result, for the present research which adopted the use of qualitative textual method, it will be quite reasonable and vital to assess these various meanings in the contexts of environmental education and leadership in establishing a holistic structure that could enable educational organizations to implement competitive and environmentally enduring guidance. Qualitative methodologies match interpretative approaches since they are holistic and quality methods meant to consider the inductivity of strategies. A qualitative approach is vital because it is distinct from the techniques used in optimistic paradigms linked to science laws. In seminal research, past study defines quantitative researches that numbers are focused on the empirical results are constrained in trying to justify only why things happen without considering both in why and how things happen (Sung, 2021; Kang, 2020).

3.1. Justification for the Qualitative Textural Methodology

One of the main problems in science is whether they are using epistemology that is objectivistic or interpretative. Previous research has shown that researchers can use qualitative research if factual knowledge is needed to address research questions. In the last report, qualitative research was also preferable if questions regarding thoughts, behaviors, perceptions, beliefs, and desires are addressed. Irrespective of the procedure, the study is sufficient if it has a high certainty in the thorough definition, interpretation, and justification. For instance, a textural analysis would be integrated into the researcher's data collection to determine the topics most apparent in the report. These themes will shape the strategies for enhancing corporate leaders by technical practitioners and other forensic researchers. Furthermore, it may be necessary for researchers to demonstrate their validity adequately. In this case, the study tried to provide qualitative alternatives for educational leaders. Therefore, it is suitable for the provision of systematic research recording their understanding and support (Fürsich, 2009; Hsieh & Shannon, 2005; Richard & Kang, 2018; Woo, 2021; Madah Marzuki, Nik Abdul Majid, Azis, Rosman & Haji Abdulatiff, 2020).

3.2. Justification for the Systematic Review Methodology

In this part, the results of the study are explored, following a systematic review method. First, to understand the issue, the current author used the existing theories of environmental and educational leadership. The study issue then resulted in developing a research problem that the researcher sought to address inductively. The author collected data about the possible solutions that can be used for coding creation using Web data analysis from various selected journal papers. Then, the author coded the data and generated different topics as data solutions after obtaining and loading them into the textural analysis framework. From these, strategies were identified that education leaders could use inside their policies to boost environmental leadership (Fürsich, 2009; Hsieh & Shannon, 2005; Woo & Kang, 2020; Han, 2020). After all, for corporate practitioners seeking to align their policies priorities with digital forensics, the present research showed the following five key subjects as the most important suggestions to protect corporate crime.

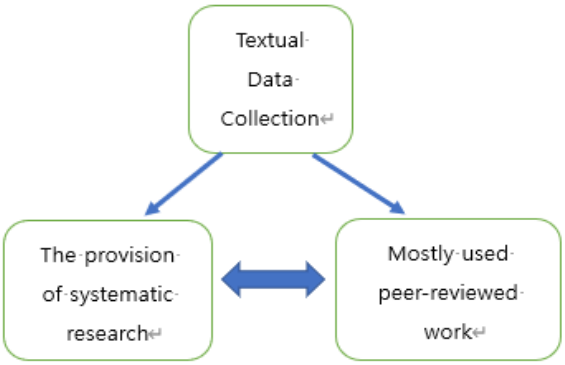

Figure 1: Overall Procedure of Literature Content Analysis

4. Findings

4.1. Solving a Problem to Anti-Forensic Techniques

Digital forensic experts' Encryption of data is one

crucial issue that digital forensic experts need to address (Dhote, 2016). The experts in digital forensics need to embrace encryption software that does not allow the readability aspect of data. The Encryption software that digital forensic have been using has also contributed to the challenge of accessibility of crime evidence by criminals, contributing to the deletion or other forms of data interference. Also, digital forensics needs to develop unique data Encryption software that experts can only use. The effort will help in ensuring that only expert digital forensic experts can access the sensitive data. There are various modern data Encryption software such as Pretty Good Privacy (PGP) as well as Rivest Shamir Adelman (RSA) (Ojha & Singh 2019). Embracing such software is essential in ensuring that the digital forensic system aims to uncover corporate crimes. Data encryption is a sensitive process in forensic science that criminals have always tried to master to understand how to read the data and alter it for their benefit (Yan, Wang, Li & Vasilakos, 2016). Developing unique software will help in achieving the privacy of sensitive information (Ojha & Singh 2019)..

Criminals are also fond of hiding data in storage space, and as such, their private information cannot easily be accessed (Al-Salehn & Al-Shamaileh, 2017). Such chunks of data are rarely invisible due to the commands and programs they have used. To uncover such trends, which often contribute to corporate crimes being unnoticed, experts in digital forensic can establish measures that will help to unlock the commands and programs that might prevent them from accessing sensitive information hidden. Another solution towards anti-forensic techniques is the control of covert channels. Covert channels often allow commination or transfer of information (Caviglione, 2021). The communication system also allows hackers to access or bypass information they are not supposed to access. The solution towards covert channels is by embracing covert analysis. The covert analysis will help the digital forensic have a new operating system, which will also help secure the sensitive data or information for purposes of uncovering criminal activities. By addressing these challenges, digital forensic will manage to safeguard its information from unauthorized intruders.

4.2. Cloud Computing Technique

The solution on cloud computing is also critical in overcoming the challenges that digital forensic often go through. Digital forensic experts must embrace modern cloud computing techniques in centralizing the sensitive data in a cloud system (Varghese & Buyya 2018). The modern techniques will ensure that the cloud system is secured from intruders who may want to temper sensitive information or evidence relating to a certain crime. Oftentimes, individuals who are suspected to be involved in corporate crimes are the ones who seek all manner of alternatives so that they can access the sensitive data store in the cloud system. Therefore, it is vital that in as much the digital forensic consider centralizing data in a cloud system, they also ensure that the system cannot be hacked or cracked by other individuals. Some of the modern tools that can help safeguard cloud computing are to ensure that the cloud computing system is built with s strong security features that cannot be accessed by people from outside (Matallah, Belalem & Bouamrane, 2017). Secondly, the digital forensic needs to have a back system for the cloud system's data. Cases of having data destroyed or interfered with by external individuals often undermine the effort invested in collecting the data, and as such, it causes the corporate crimes to go uncovered (Varghese & Buyya, 2018).

Another Solution that will help overcome the cloud system's challenge is to ensure that the cloud system is occasionally checked (Yu et al., 2016). The effort will help detect any unique attempts by intruders who may be planning to access the information. Failure to occasionally check the cloud system has resulted in some of the challenges related to cloud computing in managing the data collected. However, by testing the system, the digital forensic will make regular improvements hence preventing accessibility of the information by outsiders. It is also easy to detect when someone is trying to access the cloud system's data if those using it keep testing regularly. Another solution towards improving the cloud system's effectiveness is to use a redundant storage system (Yan, Li, Wang & Jia, 2018). A redundant storage system will help in ensuring that in case of system failure, the data is not lost but rather secured. These solutions are vital in ensuring that the cloud system is secured and safe for use.

4.3. Legal Frameworks and Guidelines

Establishing a solution on legal frameworks is also key in ensuring that the digital forensic effort is not undermined (Gaggioli, 2018). The Digital Forensic department is meant to help find justice by uncovering corporate crimes that often go unnoticed. Therefore, by advocating a legal framework, the Digital forensic department will provide evidence in court regarding a particular corporate criminal activity. One of the solutions that will help achieve a legal framework is the government through the judiciary to update Acts in the law that address security (Arewa, 2018). Using the same Act of law while changes in technology are being witnessed in every sector does not support development in the security sector in a country. For instance, in India, the judiciary has been ignorant in embracing changes in the security Act, hence undermining the digital

forensic sector's effort, which is always making an effort to help achieve justice to individuals, society, and the government (Drèze & Khera 2017). The availability of such securities needs to be reviewed.

A legal framework should be developed to help provide guidelines on how digital forensic experts need to collect information and present the information in the court of law as evidence (Adam, 2016). By doing so, the court system will support the noble effort of uncovering corporate crimes, which are increasingly becoming a concern, not in one country, one continent, but the entire world. Most of the evidence that has often been presented in the court of law by the digital forensic experts has encountered barriers of not being considered. This tendency has often occurred without reasonable grounds, and as such, the effort in conducting investigations from the forensic department seems to be undermined. This aspect encourages criminals to continue committing corporate criminals as they know that even if they are presented before a court of law, the digital forensic team's available evidence shall be dismissed by the court on the grounds of its illegitimacy.

4.4. Solution on Data Collection

When addressed, data collection is another issue that will help the digital forensic meet its goals in the industry. Some of the challenges that need fixing are the legitimacy of the collection process, the problem of anti-forensic technique, and high volumes of data (Mir, 2016). These challenges can be addressed in various ways to help achieve the goal of digital forensic. Rather than relying on one source for data collection, digital forensic experts need to diversify their sources of evidence to help achieve quality evidence. For instance, evidence obtained from one source may be considered to be biased by some opinions. However, having a guideline on collecting evidence from different sources will help enrich the quality of the evidence obtained by the digital forensic team or experts. The problem of anti-forensic techniques has also undermined the digital forensic effort, hence pausing a challenge in the safety of data collection. By strategizing on overcoming anti-forensic techniques (Wani, 2021), digital forensic will manage to uncover corporate crimes that continue to be witnessed. Developing software that provides security in data collection will help achieve quality data collected by the team. Having better software in data collection will also ensure that sensitive information on corporate crimes is collected safely and used for the intended purpose. The Digital Forensic team also needs to incorporate the cloud environment as it offers a diverse source of data from which relevant pieces of evidence can be collected (Miranda Lopez, Moon & Park, 2016). The issue of high data volume has also been a challenge, especially in storing the data. Studies show that as the data volume increases, the incidences of corporate crimes also increase, and as such, there is a need to address such an issue.

4.5. Avoidance Cultural Bias

A change in technology has also affected digital forensic in several ways. To ensure that this challenge does not continue to undermine the digital forensic sector, there is a need for forensic experts to ensure they embrace and keep pace with the changing technology. Change in technology has more benefits than how the digital forensic may perceive it. For instance, in updating the current software, the company will access improved services added to the software. Often, the digital forensic has found it a burden as the new updated software fails to be compatible with the old software that has kept sensitive data for the team. The digital forensic must develop a backup of its data system to allow the software to be updated. In such a scenario, even if the data is destroyed or lost, there will be an alternative backup that will help the digital forensic team transfer the backed-up data into the new software.

Table 2: Summary of the Present Research Findings

Main Topics	The Key to the Main Factor
1. Anti-forensic Techniques	In summary, the solution of anti-forensic techniques entails using modern encryption software to help secure data.
2. Cloud Computing Technique	Digital forensic experts must embrace modern cloud computing techniques in centralizing the sensitive data in a cloud system
3. Legal Frameworks and Guidelines	Use of redundant storage system. -Ensuring the cloud system is regularly checked
4. Data Collection	Developing software that secures data during collection. -Collecting a manageable volume of data
5. Change in Technology	Embracing new technology -Offering training on new technology -Use of new software in the analysis of sensitive data

Embracing new technology in digital forensic will also improve the efficiency of the entire process of data collection. Since digital forensics focuses much on the computer-related investigation, it is vital for the experts within the sector to always remain updated in issues related to technology as such will help in achieving the primary goal of digital forensic. There is a need for initiating

training on the use of new technologies among members of the digital forensic (Karabiyik, Mousas, Sirota, Iwai & Akdere, 2019). The effort will help all members to be acquainted with vital skills brought about by the new technology. This effort is one of the most reliable in embracing and incorporating the increasingly changing digital forensic technology. When each individual is trained on using the new technology in investigating, acquiring sensitive information will become easier for the team (Zhang & Choo 2019).

5. Implication and Recommendation

Various implications can be witnessed in enforcing the above solutions. Positive implications often help motivate a process (Towler, White, Ballantyne, Searston, Martire & Kemp, 2018). The implications are positive, and as such, they help the digital forensic team achieve its primary objective, which is to store original evidence in its form as it investigates data collection, identification, and validation of electronic information to establish evidence on criminal activities from past events (Chin, Ribeiro & Rairden, 2019). According to Choi, Yu, Hyun and Kim (2019), the implication of achieving a high level of data encryption helps in safeguarding sensitive evidence for purposes of addressing crime issues. Therefore, data encryption has a positive impact on a digital forensic, and as such, it should be embraced. The implication of having reliable cloud computing will also help in centralizing the storage of data in a cloud system that serves as a backup. A legal framework has also proven essential in helping the digital forensic use the evidence obtained in the court of law. The effort will promote justice by ensuring criminals are held accountable. The framework also serves as a guideline in the investigation process.

Additionally, data collection is critical to digital forensic. According to (Quick & Choo 2016), a successful data collection process will help digital forensic uncover sensitive data that can help eliminate corporate crimes. An increasing number of corporate crimes continue to threaten the economy and society (Schell-Busey, Simpson, Rorie & Alper, 2016). For achieving justice through the investigation of digital forensic, there is a need to eradicate corporate crimes. Embracing a change in technology also positively impacts digital forensic (Karie & Karume, 2017). Studies have shown that embracing technology, new data collection tools, and analysis will help achieve a digital forensic goal (Roux et al., 2018). These implications are essential for helping to achieve the goal of digital forensic.

Prior digital forensic studies have been paid tremendous attention by corporate management team for several decade, recognizing as a significant area and experiencing the importance of digital evidence. This tool focused on firing employees and demonstrating innocence to reduce the rate of corporate crime. Nevertheless, digital forensics is a field of science that requires consistently higher standards to be maintained, and different approaches to reduce corporate crime based on the solutions presented in this study should be definitely reviewed and discussed in the future. Since the quality of the analysis tool has improved by making it available to the general public, the next step should be focused on improving confidence in the implement continuing in time toward completion of discussion, formal testing, and publication process for corporate management teams

6. Conclusion

Digital forensic, also called digital forensic science, emanates from the main branch of forensic science. As a branch of forensic science also focuses on recovering and investigating criminal incidences and materials existing in digital devices, often involving computer crime. Corporate crime or an organizational crime is an offense committed by an individual or an official in a corporate entity for organizational gain. The effects of corporate crimes may be social or economic. Corporate crimes have not been easy to control as most of those involved are elite members of the society who equally highly educated. The challenges facing forensic science can be categorized into technical challenges, legal challenges, resource Challenges. Technical challenges are related to the advancement in technology. Encryption, data hiding storage space, and covert channel are examples of the anti-forensics technique that are often causing challenges. Operating in the cloud is a technical challenge as the digital forensic departments try to address corporate crimes in organizations. Digital forensics is also facing legal challenges that are continuously affecting uncovering corporate crimes in organizations.

As corporate crime increases in rate, the data collected by digital forensics also increases. The challenge of analyzing such chunks of data requires digital forensic experts, who need various tools to analyze the data. Research shows that a change in technology such as the operating system, computer application software, hardware, and digital evidence interpretation is becoming a challenge as the new computer application software is not compatible with older software's data structure. Encryption of data by digital forensic is one crucial issue that, when addressed, serves as a solution to digital forensic challenges. The solution on cloud computing is also critical in overcoming the challenges that digital forensic often go through. Addressing data collection and changes in technology can also help bring change.

References

Adam, C. (2016). *Forensic Evidence in Court: Evaluation and Scientific Opinion.* Hoboken, NJ: John Wiley & Sons.

Al-Saleh, M. I., & Al-Shamaileh, M. J. (2017). Forensic artefacts associated with intentionally deleted user accounts. *International Journal of Electronic Security and Digital Forensics, 9*(2), 167-179.

Arewa, A. (2018). Borderless crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime, 25*(1), 619-631.

Årnes, A. (2017). *Digital forensics.* John Wiley & Sons.

Caviglione, L. (2021). Trends and Challenges in Network Covert Channels Countermeasures. *Applied Sciences, 11*(4), 1641.

Chin, J. M., Ribeiro, G., & Rairden, A. (2019). Open forensic science. *Journal of Law and the Biosciences, 6*(1), 255-288.

Choi, J., Yu, J., Hyun, S., & Kim, H. (2019). Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. *Digital Investigation, 28*(April), S50-S59.

Dhote, C. A. (2016). Homomorphic encryption for security of cloud data. *Procedia Computer Science, 79*, 175-181.

Drèze, J., & Khera, R. (2017). Recent social security initiatives in India. *World Development, 98*(October), 555-572.

Elsadig, M. A., & Fadlalla, Y. A. (2016). Survey on covert storage channel in computer network protocols: detection and mitigation techniques. International *Journal of Advances in Computer Networks and Its Security, 6*(3), 11-17.

Fürsich, E. (2009). In defense of textual analysis: Restoring a challenged method for journalism and media studies. *Journalism studies, 10*(2), 238-252.

Gaggioli, G. (2018). International Humanitarian Law: The legal framework for humanitarian forensic action. *Forensic science international, 282*(January), 184-194.

Harshany, E., Benton, R., Bourrie, D., & Glisson, W. (2020). Big Data Forensics: Hadoop 3.2. 0 Reconstruction. *Forensic Science International: Digital Investigation, 32*(April), 300909.

Han, S. (2020). Theoretical Interdisciplinarity between Psychological Marketing Practice and Woman's Narcissism in Distribution Channels. *Journal of Distribution Science, 18*(12), 101-109.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research, 15*(9), 1277-1288.

Kang, E. (2020). The Relationship between Reinforcement of Employee's Customer-Centric Behavior and Employee Motivation Factors. *Advances in Social Sciences Research Journal, 7*(7), 338-347.

Karie, N. M., & Karume, S. M. (2017). Digital forensic readiness in organizations: Issues and challenges. The *Journal of Digital Forensics, Security and Law: JDFSL, 12*(4), 43-53.

Karabiyik, U., Mousas, C., Sirota, D., Iwai, T., & Akdere, M. (2019). *A virtual reality framework for training incident first responders and digital forensic investigators. In International Symposium on Visual Computing* (pp. 469-480), New York, USA: Springer.

Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences, 50*(5), 552-591.

Kumar, A., Kansal, A., & Singh, K. (2019). An improved anti-forensic technique for JPEG compression. *Multimedia Tools and Applications, 78*(18), 25427-25453.

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. International *Journal of Criminal Justice Sciences, 12*(2), 196-207.

Madah Marzuki, M., Nik Abdul Majid, W. Z., Azis, N. K., Rosman, R., & Haji Abdulatiff, N. K. (2020). Fraud Risk Management Model: A Content Analysis Approach. *The Journal of Asian Finance, Economics, and Business, 7*(10), 717-728.

Matallah, H., Belalem, G., & Bouamrane, K. (2017). Towards a new model of storage and access to data in big data and cloud computing. *International Journal of Ambient Computing and Intelligence, 8*(4), 31-44.

Miranda Lopez, E., Moon, S. Y., & Park, J. H. (2016). Scenario-based digital forensics challenges in cloud computing. *Symmetry, 8*(10), 107.

Mir, S. S., Shoaib, U., & Sarfraz, M. S. (2016). Analysis of digital forensic investigation models. International *Journal of Computer Science and Information Security, 14*(11), 292-301.

Nantharath, P., Laochankham, S., Kamnuasilpa, P., & Kang, E. (2020). Fiscal Decentralization and Economic Growth in Thailand: A Cross-Region Analysis. *International Journal of Financial Research, 11*(1), 147-156.

Ojha, V., & Singh, R. (2019). Pretty Good Privacy: An e-mail Security Protocol. International *Journal on Future Revolution in Computer Science & Communication Engineering, 5*(5), 80-83.

Omolaye-Ajileye, A. (2016). Admissibility of Electronic Evidence in Civil and Criminal Proceedings. In *2016 Refresher Course for Judicial Officers on Current Trends in Law and Administration of Justice* (pp. 1–32). Abuja, Nigeria: National Judicial Insitute (NJI).

Park, K. J., Park, J. M., Kim, E. J., Cheon, C. G., & James, J. I. (2017). Anti-forensic trace detection in digital forensic triage investigations. *Journal of Digital Forensics, Security and Law, 12*(1), 31-40.

Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: digital forensic images and electronic evidence. *Cluster Computing, 19*(2), 723-740.

Richard, J., & Kang, E. (2018). Culture, Competencies and Compensation: A Framework for Pay for Performance Incentives. American *Journal of Management, 18*(4), 33-48.

Roux, C., Ribaux, O., & Crispino, F. (2018). Forensic science 2020–the end of the crossroads? Australian *Journal of Forensic Sciences, 50*(6), 607-618.

Schell-Busey, N., Simpson, S. S., Rorie, M., & Alper, M. (2016). What works? *A systematic review of corporate crime deterrence. Criminology & Public Policy, 15*(2), 387-416.

Sung, I. (2021). Interdisciplinary Literature Analysis between Cosmetic Container Design and Customer Purchasing Intention. *The Journal of Industrial Distribution & Business, 12*(3), 21-29.

Towler, A., White, D., Ballantyne, K., Searston, R. A., Martire, K. A., & Kemp, R. I. (2018). Are forensic scientists' experts? *Journal of Applied Research in Memory and Cognition, 7*(2), 199-208.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems, 79*(Part 3) 849-861.

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research, 17*(2), 183-194.

Wani, M. A., AlZahrani, A., & Bhat, W. A. (2020). File system anti-forensics–types, techniques and tools. *Computer Fraud & Security, 2020*(3), 14-19.

Wani, M. A. (2021*). Privacy Preserving Anti-Forensic Techniques. In Multimedia Security* (pp. 89-108), Singapore: Springer.

Warren, C., El-Sheikh, E., & Le-Khac, N. A. (2018). *Privacy preserving Internet browsers: Forensic analysis of Browzar. In Computer and network security essentials* (pp. 369-388). New York, USA: Springer.

Woo, E. J. (2021). The Relationship between Green Marketing and Firm Reputation: Evidence from Content Analysis. *The Journal of Asian Finance, Economics and Business, 8*(4), 455-463.

Woo, E. J., & Kang, E. (2020). Environmental Issues As an Indispensable Aspect of Sustainable Leadership. *Sustainability, 12*(17), 7014.

Yan, H., Li, X., Wang, Y., & Jia, C. (2018). Centralized duplicate removal video storage system with privacy preservation in iot. *Sensors, 18*(6), 1814.

Yan, Z., Wang, M., Li, Y., & Vasilakos, A. V. (2016). Encrypted data management with deduplication in cloud computing. *IEEE Cloud Computing, 3*(2), 28-35.

Yu, Y., Xue, L., Au, M. H., Susilo, W., Ni, J., Zhang, Y., & Shen, J. (2016). Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems, 62*(September), 85-91.

Zhang, X., & Choo, K. K. R. (2019). *Digital Forensic Education: An Experiential Learning Approach* (Vol. 61), New York, USA: Springer.

Zubańska, M. (2018). Old Forensic Evidence, Contemporary Resources of Forensic Science and the Police X-Files—Crime Is Not an Abstract and Theoretical Entity Out of Touch with Reality. *Internal Security, 10*(1), 107-124.