Prestieesci Research Review

A STUDY ABOUT ROLE OF COMPUTERS IN DIGITAL FORENSICS FOR BUSINESS DURING DISASTER AND CYBER CRISIS: A COMPREHENSIVE STUDY

Peng Jinyin, Divya Midhunchakkaravarthy

Lincoln University College, 47301 Petaling Jaya, Selangor D. E., Malaysia.

Corresponding author: Peng Jinyin, Lincoln University College, 47301 Petaling Jaya, Selangor D. E., Malaysia, Email: 274134337@qq.com

ABSTRACT

To discover criminal activities, digital forensics is crucial in researching and analyzing digital evidence. Computers are now essential in digital forensics because to the ever-increasing complexity and volume of digital data. In this article, the researcher will look at the many ways computers have helped in digital forensics, focusing on areas like evidence gathering, analysis, and presentation. As computing power has increased, forensic investigators have access to more effective methods for gathering, storing, and analyzing digital evidence. There are possibilities and difficulties for digital forensics professionals brought about by developments in data storage and retrieval and the proliferation of networked devices. Data recovery, forensic analysis software, and machine learning are some of the computational technologies discussed in this study as crucial in improving the efficiency and precision of investigations. In addition, it delves into the legal and ethical aspects of digital forensics and how computers play a role in this field. This study highlights the relevance of multidisciplinary collaboration and continuous technical breakthroughs in addressing cyber threats and ensuring the integrity of digital investigations by clarifying the symbiotic link between computers and digital forensics. Computers' function in digital forensics is the foundation of the paper. As the world becomes more digital, all of these sectors are incorporating digitalisation into their operations.

Digitalization has greatly improved the efficiency and speed of the working operations. A computer or other system is all that is needed to utilize digitalization.

Keywords: Computer, Digital world, Forensic world, Cyber crisis.

INTRODUCTION

Cybercrime has increased dramatically in this age of pervasive digital technology, calling for new approaches to investigation to keep up with the ever-changing nature of the internet. Collecting, analyzing, and preserving electronic evidence is known as digital forensics, and it has become an essential discipline in the fight against cyber threats. Computers are crucial to this investigative skill since they are the arena for cybercrimes and the foundation of forensic analysis. With the proliferation of digital footprints across many devices and platforms, forensic practitioners are increasingly reliant on advanced computational approaches. This study delves into the significant role that computers play in digital forensics, illuminating how they aid in gathering evidence, analyzing it, and conducting the investigation. The researcher looks at how tech and forensics work hand in hand, and how a deep knowledge of computers is essential for deciphering the complex network of digital evidence (Beebe, 2019). Pursuing justice and protecting digital integrity requires a grasp of the dynamic interaction between computers and digital forensics, which is becoming more important as the digital domain evolves. The worldwide use of the Internet and related technologies has skyrocketed this century. The increase in the worldwide occurrence of digital crimes, frequently referred to as e-crimes, is clearly associated with this growth. The prevention, identification, investigation, and prosecution of connected offences are confronted with new obstacles by these digital crimes (Mohammad, 2020).

The incredibly complex nature of cybercrime has given rise to a new subfield of forensic science in computer forensics. Emerging as a field of study, computer forensics seeks to identify these crimes and collect digital evidence that may be presented in court by means of computer inquiry and analysis. A plethora of fascinating and difficult unsolved computer security and cryptography challenges have arisen because of this emerging area, which integrates expertise in IT, forensics, and law. A growing number of municipal police departments are showing an interest in computer forensics. Practically every kind of enforcement operation now makes use of it for judicial competence. But there haven't been enough investments to make it as accurate as alternatives like fingerprint analysis, so it falls behind. Hence, the judicial system isn't always told the whole truth about the reliability or significance of digital evidence. Legal procedures are approached through the lens of digital forensics, which employs scientific knowledge and cutting-edge technology.

Digital forensics aims to provide a systematic examination and organize a recorded chain of proof and evidence in order to ascertain the precise events that transpired on a digital device (Ashraf et al., 2021).

BACKGROUND OF THE STUDY

A more popular name for the field that would later be known as digital forensics was "computer forensics" until the late 90s (Mohammad, 2020). Law enforcement professionals with an interest in computers were the first to specialize in computer forensics. In an effort to bolster cybersecurity, data localisation, and the protection of sensitive information, the Chinese Cybersecurity Law—also known as the National People's Congress approved it—was supposedly enacted for the sake of national security. The measures are intended to successfully counteract "major risks" by the year 2026 (Ahmed et al., 2021). Among the steps taken are data security training and emergency simulations mimicking ransomware attacks. More than 45,000 businesses in the manufacturing sector will get their applications. To start off their careers, most cyber security experts go for a bachelor's degree in the subject, or one closely connected, like IT or computer science. The Chinese government is stepping up its supervision and making it clear that international enterprises must adhere to local rules by merging existing legislation on VPN and data security into the cybersecurity law. Liability rules and definitions are also included in the cybersecurity legislation. The idea of military-civil fusion, which promotes cooperation and resource integration between the military and the business sector, is an important part of China's cyber strategy (Ghamdi, 2021).

PURPOSE OF THE RESEARCH

Organisations may enhance their reaction to cybercrime interruptions by adjusting their disaster recovery policies and practices. This was the goal of this qualitative Delphi research. To develop a new framework for responses, our qualitative approach focused on individuals engaged in IT disaster recovery. The interviews of twenty-two individuals with a minimum of five years' experience in five different disaster recovery situations allowed us to identify patterns or themes. Companies' present IT disaster recovery frameworks for getting back to normal operations were the main focus of the inquiry. We developed a new model to help you understand how extra cybersecurity or computer incident response frameworks may affect your IT disaster recovery operations. The researcher opted for the Delphi approach over a case study or another qualitative research technique because students wanted to learn how to improve the disaster response process and what factors influence specific responses.

LITERATURE REVIEW

“The preservation, identification, extraction, interpretation, and documentation of computer evidence, including the rules of evidence, legal processes, evidence integrity, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found” (Shaer et al., 2020). Each of the five subfields of digital forensics—computer, network, mobile device, memory, and email—focuses on a specific kind of digital evidence. Alghamdi states that the field of computer forensics is concerned with the acquisition, preservation, retrieval, and presentation of data that has undergone electronic processing and storage on digital media (Alhamdi, 2021). Network forensics is the study of how to use scientifically proven methods to gather, combine, identify, scrutinise, correlate, analyse, and record digital evidence from various digital sources that are currently processing and transmitting data. The goal is to find out what happened during unauthorised attempts to corrupt, compromise, or disrupt system components, or how to recover from such attacks. According to Alkatheiri et al. (2021), mobile device forensics is a subfield of digital forensics that aims to retrieve digital evidence from mobile devices in a secure and dependable manner by using known procedures.

RESEARCH QUESTION

1. What is the role of computers in data recovery during digital forensics?

RESEARCH METHODOLOGY

Quantitative research refers to studies that examine numerical readings of variables using one or more statistical models. The social environment may be better understood via quantitative research. Quantitative approaches are often used by academics to study problems that impact particular individuals. Objective data presented in a graphical format is a byproduct of quantitative research. Numbers are crucial to quantitative research and must be collected and analyzed in a systematic way. Averages, predictions, correlations, and extrapolating findings to larger groups are all possible with their help.

Research design: In order to analyse quantitative data, SPSS version 25 was used. When analysing the statistical association, the odds ratio and 95% confidence interval were used to determine its direction and size. A statistically significant threshold was suggested by the researchers at $p < 0.05$. The primary features of the data were identified by a descriptive analysis. Mathematical, numerical, or statistical evaluations using quantitative methodologies are often used for data gathered from surveys, polls, and questionnaires, or by modifying existing statistical data using computing tools.

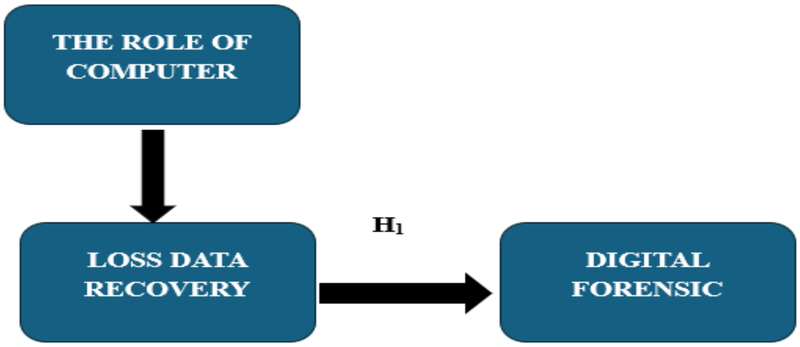
Sampling: After pilot research with 20 Chinese Researcher, 1100 Rao-soft pupils were included in the final Investors. Male and female Researcher were picked at random and then given a total of 1455 surveys to fill out. A total of 1253 questionnaires were used for the calculation after 1300 were received and 47 were rejected due to incompleteness.

Data and Measurement: A questionnaire survey functioned as the primary data collection instrument for the investigation. The survey had two sections: (A) General demographic information and (B) Responses on online and non-online channel factors on a 5-point Likert scale. Secondary data was obtained from many sources, mostly on internet databases.

Statistical software: The statistical analysis was conducted using SPSS 25 and MS-Excel.

Statistical Tools: To grasp the fundamental character of the data, descriptive analysis was used. The researcher is required to analyse the data using ANOVA.

CONCEPTUAL FRAMEWORK



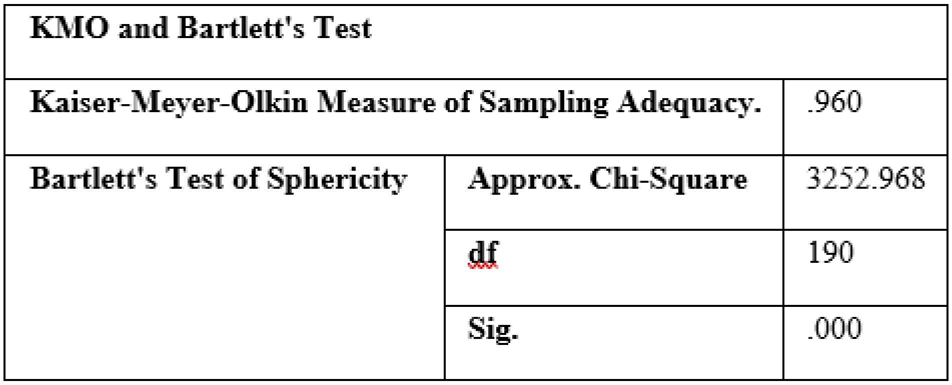
RESULT

Factor analysis

One typical use of Factor Analysis (FA) is to verify the existence of latent components in observable data. When there are not easily observable visual or diagnostic markers, it is common practice to utilize regression coefficients to produce ratings. In FA, models are essential for success. Finding mistakes, intrusions, and obvious connections are the aims of modelling. One way to assess datasets produced by multiple regression studies is with the use of the Kaiser-Meyer-Olkin (KMO) Test. They verify that the model and sample variables are representative. According to the numbers, there is data duplication. When the proportions are less, the data is easier to understand. For KMO, the output is a number between zero and one. If the KMO value is between 0.8 and 1, then the sample size should be enough. These are the permissible boundaries, according to Kaiser: The following are the acceptance criteria set by Kaiser:

A dismal 0.050 to 0.059, subpar 0.60 to 0.69 Middle grades often range from 0.70 to 0.79. Exhibiting a quality point score between 0.80 and 0.89. They are astonished by the range of 0.90 to 1.00. Table 1: KMO and Bartlett's Test for Sampling Adequacy Kaiser-Meyer-Olkin measurement: .960 The outcomes of Bartlett's test of sphericity are as follows: Approximately chi-square degrees of freedom = 190 significance = 0.000 This confirms the legitimacy of claims made just for sampling purposes. Researchers used Bartlett's Test of Sphericity to ascertain the significance of the correlation matrices. A Kaiser-Meyer-Olkin value of 0.960 indicates that the sample is sufficient. The p-value is 0.00 according to Bartlett's sphericity test. A positive outcome from Bartlett's sphericity test indicates that the correlation matrix is not an identity matrix.

Table: KMO and Bartlett's



KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.960
Bartlett's Test of Sphericity	**Approx. Chi-Square**	3252.968
	df	190
	Sig.	.000

The overall importance of the correlation matrices was also validated by Bartlett's Test of Sphericity. The Kaiser-Meyer-Olkin sampling adequacy is 0.960. Utilising Bartlett's sphericity test, researchers obtained a p-value of 0.00. A notable result from Bartlett's sphericity test indicated that the correlation matrix is not valid.

- **Independent variable**

Role of the Computer:

Nowadays, researchers depend on computers in some manner for almost every task, whether it's personal (like managing a savings account) or professional (like selling a product or service). The increasing reliance on computers has led to the provision of computer-based services by various types of organisations and businesses, both large and small. In addition, corporations now have more options than ever before for conducting business, transferring payments, and delivering services thanks to the proliferation of multimedia, electronic service networks, and other forms of communication technology (Alzubaidi, 2021). Businesses are becoming more autonomous because of computers' ability to automate processes. With the use of computers, most tasks can now be automated, eliminating the need to employ human labor for every task. Everything is automated, from purchasing tickets to making high-end automobiles. Since many companies now operate only online, centralizing their inventory might be more efficient than opening physical locations in each area. Many workers are unnecessary (Amir, 2020).

- **Factor**

Loss data recovery:

What business data recovery is all about is getting data that has been destroyed, lost, accidentally deleted, or is otherwise inaccessible back onto a server, computer, mobile device, storage device, or even a new device if the old one stops operating. The data is usually restored from a separate, off-site copy (Ashraf et al., 2021). Data recovery success is directly proportional to the freshness of the backup copy. A backup and restore strategy that achieves set data recovery objectives is usually part of a larger disaster recovery plan. This is necessary for data recovery in order to prevent an unbearable loss of data or the entire shutdown of activities due to data loss (Aziz & Amtual, 2019).

- **Dependent variable**

Digital Forensic:

Forensic science includes digital forensics. Not only may it aid in civil and criminal investigations, but it is also used to probe cybercrimes. As an example, digital forensics may be used by cybersecurity teams to track down malware attackers and by law enforcement authorities to examine evidence retrieved from a suspect's devices in a murder investigation. Because digital evidence is treated like any other kind of evidence, digital forensics has many uses. Like how authorities adhere to certain protocols when collecting physical evidence from a crime scene, investigators specializing in digital forensics adhere to a rigorous protocol when dealing with digital evidence to prevent any kind of manipulation (Cheng et al., 2020). There is a lot of confusion between digital forensics and computer forensics. In contrast to computer forensics, which focusses on computing devices like PCs, tablets, smartphones, and other devices with central processing units (CPUs), digital forensics formally includes collecting evidence from any digital device. A young field in cybersecurity known as digital forensics and incident response (DFIR) combines computer forensics with incident response operations to speed up the cleaning process after cyber-attacks without damaging any connected data evidence (Dash et al., 2021).

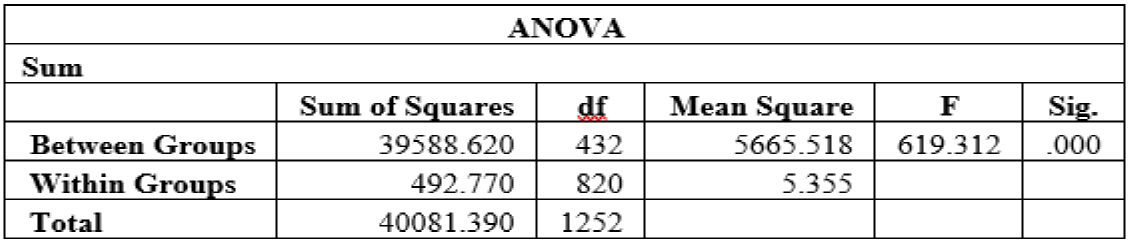
- **Relationship between digital forensic and loss data recovery**

Criminals in the modern digital era often erase potentially damning information from their gadgets to disguise their tracks. Nevertheless, specialists in digital forensics have the knowledge and tools to retrieve this apparently deleted data. As expert witnesses in computer forensics, they use a variety of techniques to recover and examine data. Imaging a disc entail making a replica of the whole thing, bit by piece. The authenticity of the evidence can be maintained as this copy can be examined and changed without impacting the original device. To keep the data admissible in court, this method makes sure that it doesn't change in any way from the original. File carving involves locating file signatures, such as headers and footers, to retrieve missing or corrupted files from a device's image (Beechey et al., 2021). When all hope is gone, this procedure is priceless for retrieving lost data. Forensic specialists may nevertheless retrieve vital data in the absence of metadata by looking for certain patterns or signatures (Ashraf et al., 2021).

H01 : There is no significant relationship between loss data recovery and digital forensic.

H1: There is a significant relationship between loss data recovery and digital forensic.

Table 2: H_1 ANOVA Test



ANOVA					
Sum					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	39588.620	432	5665.518	619.312	.000
Within Groups	492.770	820	5.355		
Total	40081.390	1252			

This investigation yields remarkable results. The F value is 615.212, achieving significance with a p-value of .000, which is below the .05 alpha threshold. This means “H1: There is a significant relationship between loss data recovery and digital forensic.” The alternative hypothesis is accepted, whereas the null hypothesis is rejected.

DISCUSSION

The research meets a need in literature by focusing on the agreement among cybersecurity and IT disaster recovery experts. Experts predict that this trend will continue to worsen. While cybercrime poses new risks to businesses, conventional disaster recovery methods still use historical data to prepare for and recover from events like power outages, floods, and fires (Bullock et al., 2021). Those in positions of authority should work together to provide a seamless transition between cybersecurity and disaster recovery. Responders and planners for IT disaster recovery might utilise some training in general or specialised cybersecurity measures to help them be better prepared for both the planning stage and the conceptual awareness they'll need during an interruption caused by cybercrime. Cybersecurity training has the potential to shed light on hitherto unseen efforts to mitigate risk. According to Cao, companies may enhance their capacity to recover from disruptions to their operations more rapidly and effectively if they investigate methods to include more cybersecurity into the disaster recovery lifecycle. (Cao et al., 2019).

CONCLUSION

Finding ways to mitigate the impact of cybercrime on disaster recovery initiatives was the driving force behind this study, which drew on the experiences and insights of scholars in the field, first responders to such incidents, and cybersecurity specialists. The study participants emphasized the need of including cybersecurity risks into the disaster recovery process, even if the concept was initially based on emergency management concepts in response to natural catastrophes. The paper suggests that in order for organisations to be better prepared, manage risks, learn from their mistakes, and raise responder awareness, they should include cybersecurity expertise into their disaster recovery plans. An increase in cybersecurity education could pave the way for a more effective response to disaster recovery after a computer crime interruption (Chen et al., 2021). An additional area of investigation in this study was the potential for integrating disaster recovery procedures with cybersecurity frameworks. Adding the incident response processes, defensive measures, and monitoring included in popular cybersecurity frameworks to existing IT disaster recovery plans and procedures is a simple but effective solution.

When asked about the benefits of merging the two ideas, participants in this study mentioned them in many places. Based on the findings of this research, organisations should enhance their disaster recovery programs by integrating a cybersecurity framework and look at methods to increase cybersecurity expertise within their disaster recovery teams. (Chandra & Snowe, 2020).

REFFERENCE

1. N. Beebe, Digital forensic research: The good, the bad and the unaddressed. In IFIP International Conference on Digital Forensics (pp. 17-36). Springer, Berlin, Heidelberg. (2019).
2. SM. Mohammad, Security and Privacy Concerns of the 'Internet of Things' (IoT) in IT and its Help in the Various Sectors across the World International Journal of Computer Trends and Technology 2020.
3. Ahmed Jamal A., et al. A review on security analysis of cyber physical systems using machine learning Mater. Today: Proc. (2021)
4. Al-Ghamdi M.I. Effects of knowledge of cyber security on prevention of attacks Mater. Today: Proc. (2021)
5. Shaer D., et al. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens Eur. J. Med. Chem., 208 (2020), Article 112791
6.

   Alghamdi M.I. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia Mater. Today: Proc. (2021)
7. Alkatheiri M.S., Chauhdary S.H., Alqarni M.A. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications Sustain. Energy Technol. Assess., 45 (2021), Article 101219
8. Alzubaidi A. Cybercrime awareness among Saudi nationals: Dataset Data Brief, 36 (2021), Article 106965
9. Amir M., Givargis T. Pareto optimal design space exploration of cyber-physical systems Internet Things, 12 (2020),Article 100308 Ashraf J., et al. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities Sustainable Cities Soc., 72 (2021), Article 103041
10. Aziz A.A., Amtul Z. Developing Trojan horses to induce, diagnose and suppress Alzheimer’s pathology Pharmacol. Res., 149 (2019), Article 104471
11. Beechey M., Kyriakopoulos K.G., Lambotharan S. Evidential classification and feature selection for cyber-threat hunting Knowl.-Based Syst., 226 (2021), Article 107120
12. Bullock J.A., Haddow G.D., Coppola D.P. Cybersecurity and critical infrastructure protection
13. Bullock J.A., Haddow G.D., Coppola D.P. (Eds.), Introduction to Homeland Security (sixth ed.), Butterworth-Heinemann (2021), pp. 425-497

14. Cao Y., et al. A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification Comput. Secur., 87 (2019), Article 101478
15. Chandra A., Snowe M.J. A taxonomy of cybercrime: Theory and design Int. J. Account. Inf. Syst., 38 (2020), Article 100467
16. Chen J.-K., et al. Cyber deviance among adolescents in Taiwan: Prevalence and correlates
17. Child. Youth Serv. Rev., 126 (2021), Article 106042
18. Cheng S., et al. A new hybrid solar photovoltaic/phosphoric acid fuel cell and energy storage system; Energy and exergy performance Int. J. Hydrogen Energy (2020)
19. Dash N., Chakravarty S., Satpathy S. An improved harmony search based extreme learning machine for intrusion detection system Mater. Today: Proc. (2021)