Prestieesci Research Review

DEPTH ANALYSIS OF THE FUNCTIONS OF COMPUTERS IN DIGITAL FORENSICS AS THEY RELATE TO ORGANISATIONS IN TIMES OF CRISIS AND DISASTER

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

Digitalisation is booming these days, and everyone from individuals to large corporations is using it to their advantage. There has to be some kind of digital system that allows us to do more in less time if researcher are to achieve this goal. On top of that, the researcher utilise social media sites for fun. The researcher don't see anything wrong with this, but researcher need to be cautious with our systems and social media since crime is on the rise along with digitisation. Installing software that protects against cyber attacks is a must. There are a variety of assault strategies, and The researcher need to be aware of them. In essence, this presentation will centre on the field of digital forensics and the function that computers play in it, which will assist us in the event of an assault. Anxieties about China's potential digital infrastructure collapse and the resulting loss of competitive edge have gotten out of hand. Every area where the West claims a cyber threat from China has significant Western advantages and major Chinese weaknesses. Prioritising political information control above technical cyber defence has led to China's networks being less efficient economically and more vulnerable to foreign infiltration. China may stealthily penetrate overseas targets as well, but it's unclear how well it can use stolen data, particularly in the most competitive parts of the value chain where the US has a stronghold. Discovering and making sense of data stored in digital form is known as digital forensics. Through systematic collection, identification, and validation of digital material, the technique aims to restore historical events while preserving evidence in its most original form.

Keywords: Cyber Disaster, Cyber Security, Digital Forensics, Cyber Crime, Functions of computers.

INTRODUCTION

Focussing on the significance and function of computers within digital forensics, this research aims to illuminate the field. Cybercrime using social media is rising at an alarming rate, paralleling the expansion of the internet. Therefore, digital forensics has developed as a reaction to these cybercrimes (Xu et al., 2020). As a branch of forensic science, digital forensics is concerned with the investigation of cybercrime by the methodical investigation and recovery of data or evidence stored in electronic devices. Everything from data stored on your computer or mobile device to data sent over a private network might be subject to digital forensics. Digital forensics was formerly known as computer forensics. Evidence gathered via digital forensics may help solve both traditional and non-traditional crimes. The basic idea behind this procedure is to keep every evidence as original as possible while the inquiry is underway. To determine what happened on the digital device, digital forensics primarily aims to conduct a methodical investigation while arranging a documented chain of proof and evidence. Given the current state of cybercrime and the importance of computer security, it is imperative that computer workers have a solid grasp of the technologies used in digital forensics. The essentiality of doing digital forensics in a legitimate and efficient manner is the subject of this study. In the field of forensic science known as "digital forensics," the goal is to discover, collect, analyse, analyse, and report on information kept in digital form. Almost every illegal conduct involves some kind of electronic evidence, and the assistance of digital forensics experts is vital to the enforcement of laws (Wang et al., 2021).

BACKGROUND OF THE STUDY

'Computer forensics' was the widespread name for the field that would later be known as digital forensics until the late 1990s. Law enforcement professionals with an interest in computers were the first to specialise in computer forensics. In an effort to better safeguard sensitive information, localise data, and enhance cybersecurity, the Chinese Cybersecurity Law—officially known as the National People's Congress Cybersecurity Law—was enacted by the National People's Congress. Plans are in place to successfully counteract "major risks" by 2026's conclusion. Data security training and emergency simulations mimicking ransomware assaults are two steps in the right direction. More than 45,000 businesses in the manufacturing sector will get their applications. The majority of cyber security experts started their professions after earning a bachelor's degree in the subject or one closely linked to it, like IT or computer science (Singh et al., 2019). The Chinese government has strengthened its supervision and emphasised the requirement of international enterprises complying with local legislation by merging existing laws on VPN and data security into the cybersecurity law. Liability rules and definitions are also included in the cybersecurity legislation. Chinese cyber strategy is heavily reliant on the idea of military-civil fusion, which promotes cooperation and

resource integration between the military and the commercial sector. Criminals committing cybercrimes may use an entry point that neither the cybersecurity team nor the emergency planners had considered. Computer crimes are expected to rise in tandem with the proliferation of technological gadgets used by enterprises (Sun et al., 2021).

PURPOSE OF THE RESEARCH

The purpose of this qualitative Delphi study was to provide recommendations for improving IT disaster recovery policies and processes in the event that a cybercrime disrupts a company's operations. emphasis order to create a fresh response framework, our qualitative method zeroed emphasis on those involved in IT disaster recovery. Patterns or themes were identified via the interviewing of twenty-two people with a minimum of five years' experience in five disaster recovery scenarios. The current information technology disaster recovery frameworks that companies use to go back to regular operations were the primary subject of the investigation. In order to better comprehend the potential impact of additional cybersecurity or computer incident response frameworks on IT disaster recovery operations, a new model was established Using a Delphi technique rather than a case study or other qualitative research strategy allowed the researcher to better understand how different factors affect specific responses and ultimately improve the disaster response process.

LITERATURE REVIEW

The significance of digital forensics was the main emphasis of this study thesis (Li et al.,2020). One of the many steps in digital forensics is evidence collecting, which entails gathering digital proof from various crime sites . The next step is to do a digital forensic analysis of the evidence utilising forensic toolkits, which provide data with various degrees of abstraction. By going through this procedure, researcher might unearth encrypted data as well as data that has been accidentally erased or misplaced from your device. Metadata may be extracted for analysis with the help of the program. According to , digital forensic analysis encompasses the domain of data analysis that aims to comprehend the collection of potential explanations and related logical sequences of events that describe the format of digital evidence. Proposing new ideas and concepts for the development of techniques and forensics tools in digital investigation, digital forensic process modelling has sought to provide overall progress to the field. Throughout this work, the taxonomy is shown (Springer et al., 2019). The author gives a comprehensive overview of digital forensics as well as how important it

is"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 the authenticity, validity, authenticity of, or lack thereof of computer-related evidence" (United States Coast Guard Academy, 2017).

RESEARCH QUESTION

1. What is the role of computers in identifying within digital forensics in China?

METHODOLOGY

Research design: We utilised SPSS version 25 for quantitative data analysis. One way to find out how strong of a correlation there was was to look at the odds ratio and the 95% confidence interval. According to the researchers, $p < 0.05$ was the threshold of statistical significance. To identify the most salient features of the data, a descriptive analysis was used. Data collected from surveys, polls, and questionnaires, as well as data that has already been statistically manipulated using computing tools, are often subjected to quantitative procedures, which include mathematical, numerical, or statistical approaches.

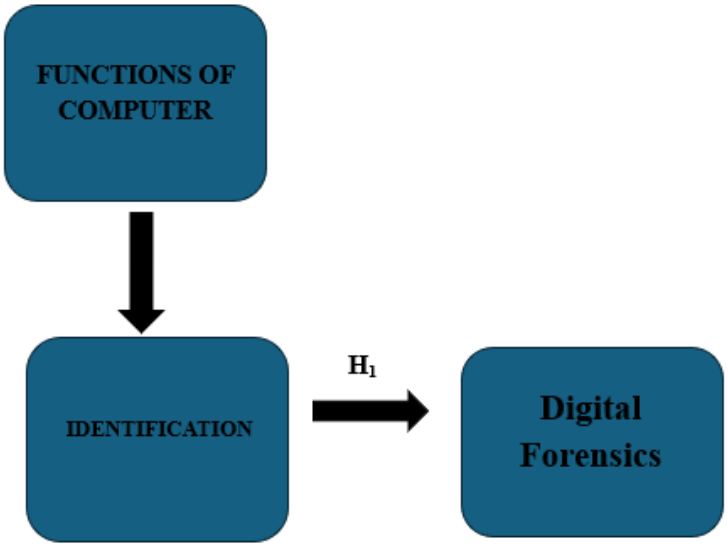
Sampling: After pilot research with 20 Chinese Researcher, 1100 Rao-soft pupils were included in the final Investors. Male and female Researcher were picked at random and then given a total of 1,455 surveys to fill out. A total of 1253 questionnaires were used for the calculation after 1300 were received and 47 were rejected due to incompleteness.

Data and Measurement: The major tool for gathering information for the study was a questionnaire survey. Part A of the survey asked for basic demographic information, while Part B asked respondents to rate various aspects of the online and offline channels using a 5-point Likert scale. A wide range of secondary sources, including internet databases, were combed through to compile the necessary information.

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 analyze 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 no easily observable visual or diagnostic markers, it is common practice to utilise 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. Average grades typically range from 0.70 to 0.79.

The quality point score ranges from 0.80 to 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 measure: .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. The Kaiser-Meyer-Olkin measure implies that a value of 0.960 signifies sample adequacy. 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 1: KMO and Bratlett's Test3

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

In other words, this proves that sample remarks are valid. Researchers used Bartlett's Test of Sphericity after confirming the significance of the correlation matrices. According to the Kaiser-Meyer-Olkin criterion, a sample is deemed good when the result is 0.960. According to Bartlett's test of sphericity, the level of significance is 0.00. A statistically significant result from Bartlett's sphericity test shows that the correlation matrix is not the same as an identity matrix.

- **INDEPENDENT VARIABLE**

Functions Of Computer:

The practice of protecting computer systems and data against harm, theft, and unauthorised access is known as cybersecurity. Serial numbers, doors and locks, and alarms are common ways that computer equipment is protected, just as they are for other costly or sensitive equipment. The four main functions of a computer are input, processing, output, and storage. A computer is a device that processes data (Li et al., 2020). Functions are independent pieces of code that are specifically created to carry out a certain task. In general, functions take in data, do some processing on it, and then return the output. It is possible to reuse a function after its construction. It is possible to call a function from inside another function. A computer is an electronic device that takes in data in digital form and processes it in accordance with a program or software's instructions to generate an output. The basic goal of computer forensics is to find, collect, store, and analyse data in a way that doesn't compromise its integrity, so it can be used effectively in court proceedings (Miller, 2020).

- **FACTOR**

IDENTIFICATION:

Stage one, "identification," involves finding important data custodians and possible devices that might have pertinent evidence or information. An important component of forensic identification is determining the likelihood that a certain individual was responsible for leaving a trace of their fingerprints or other identifying information at a crime scene. Binary information, whether saved or transferred, may be used as evidence in a court of law. You could find it on a mobile phone or a computer's hard disc. Common examples of e-crime that include digital proof include credit card fraud and child pornography. Recognition in the field of computer forensics. Gathering all of the physical objects that will be examined by computer forensics experts is the first stage. Once potential fraudsters have been identified, a thorough visual search of their workstation and surrounding area is executed to uncover any digital traces (Meserole,2022).

- **DEPENDENT VARIABLE**

DIGITAL FORENSICS:

"The process of identifying, preserving, analysing, and presenting digital evidence in a manner that is legally acceptable in any legal proceedings" is what digital forensics claims to be. One subfield of forensic science known as "digital forensics" deals specifically with electronic data and how to locate, get, process, analyse, and report

on it. Digital forensics assistance is vital for police investigations since electronic evidence is present in almost all illegal acts. One subfield of forensic science known as "digital forensics" deals specifically with the examination and retrieval of evidence pertaining to cybercrime from digital devices. Digital forensics was formerly used interchangeably with computer forensics. Research into all gadgets capable of storing digital data has now broadened its scope. It wasn't until the 1990s that the phrase "computer crime" became widely used, despite the fact that the first incidence was documented in 1978 and the Florida Computer Act followed (Horan & Saiedian, 2021). Nationwide strategies for digital forensics did not materialise until the very beginning of the current millennium. In digital forensics, evidence is found, stored, examined, and recorded in a digital format. In the event that proof must be shown in a legal proceeding, this is accomplished. Investigational data archiving entails keeping, analysing, retrieving, and conserving digital information. Devices such as laptops, smartphones, smart home appliances, car navigation systems, and electronic door locks are part of this category. The collection, analysis, and preservation of evidence is the process's end objective in digital forensics (Baror et al.,2021).

RELATIONSHIP BETWEEN IDENTIFICATION AND DIGITAL FORENSICS:

It is often believed that digital forensics is exclusively applicable in computer-related settings. However, its societal influence is far greater (Baker et al., 2020). The pervasiveness of computers and other electronic devices has made digital evidence indispensable in the investigation and resolution of many online and offline legal disputes and crimes. When a data breach occurs, digital forensics may help identify the perpetrators and determine how the breach occurred. Evidence gathered via digital forensics may aid in the identification and prosecution of offences such as corporate fraud, embezzlement, and extortion.When used to a business setting, digital forensics may help find and investigate breaches in both cyber and physical security. As a standard component of incident response, digital evidence is used to confirm the occurrence of a breach, identify the source and individuals responsible for the threat, eliminate the danger, and provide legal teams and law enforcement with proof. For digital forensics to work, businesses need a centralised system to handle logs and other digital evidence, a sufficient retention term, and security measures to prevent manipulation, unauthorised access, or unintentional loss. incidents when credentials are attempted to be stolen or accounts are taken over. Both internal company accounts and customer accounts that the organisation handles are susceptible to these kinds of threats (Delerue, 2019).

H01: There is no significant relationship between Identification and Digital Forensics.

H1: There is a significant relationship between Identification and Digital Forensics.

Table 2: H_1 ANOVA Test

ANOVA					
Sum					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	39588.620	356	5665.518	615.212	.000
Within Groups	492.770	896	5.355		
Total	40081.390	1252			

In this study, the result is significant. The value of F is 615.212, which reaches significance with a p-value of .000 (which is less than the .05 alpha level). This means the "H1: There is a significant relationship Policies and Chinese Financial Market" is accepted and the null hypothesis is rejected.

DISCUSSION

Through an emphasis on the consensus of cybersecurity and IT disaster recovery specialists, my study fills a knowledge vacuum about IT disaster recovery. A growing number of unforeseen computer crimes are disrupting organisations worldwide, and experts are projecting that this trend will only get worse (Korzachenko & Cherniavskyi, 2020). Computer crimes provide new hazards to organisations, yet traditional disaster recovery relies on past data to help with planning and restarting systems after power outages, floods, or fires (Chen et al.,2019). Cybersecurity and disaster recovery should be closely coordinated by those in charge of making important decisions. Both the preparation training IT disaster recovery planners and responders in general or specialised cybersecurity measures may boost conceptual awareness during an interruption caused by computer crimes and the phase of the recovery process. Research by (Layton, 2020) suggests that cybersecurity awareness may shed light on previously unanticipated risk management activities. Organisations should look for ways to include more cybersecurity into the disaster recovery lifecycle to improve their ability to recover quickly and efficiently from business interruptions.

CONCLUSION

This research study sought to determine ways to lessen the effect of cybercrime on disaster recovery programs by consulting with cybersecurity experts, persons who have reacted to catastrophes, and professors in the subject. While disaster recovery was first developed to address natural catastrophes using emergency management concepts (Wang et al., 2024) the participants in the study emphasised the need of expanding the approach to include cybersecurity risks. Based on the findings, businesses should include cybersecurity expertise into their disaster recovery plans to better prepare for and manage risks, as well as to share lessons learnt and raise responder awareness. A better disaster recovery reaction after a computer crime disruption should be possible as a result of a greater knowledge of cybersecurity. The feasibility of combining disaster recovery processes with cybersecurity frameworks was another focus of this research. Current IT disaster recovery plans and procedures may be simply supplemented by including the monitoring, defensive controls, and incident response processes included in popular cybersecurity frameworks. 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.

REFERENCE

2. Xu, K., Wu, D., & Yang, Z. (2020). Network information security and its relationship with information integrity: A review of technological and management perspectives. Cybersecurity Journal, 5(3), 120-132.
3. Wang, S., Lin, M., & Chen, Z. (2021). Protecting information confidentiality in the era of digital transformation. Journal of Information Privacy and Security 17(2), 125-139.
4. Singh, P., & Singh, N. (2019). Cybersecurity risks and countermeasures: A comprehensive review. International Journal of Computer Applications, 113(11), 1-10.
5. Li, H., & Zhang, Y. (2020). Information availability and network security: Ensuring system uptime in the face of threats. Cybersecurity, 3(1), 14-22.
6. Zhou, H., Wang, Q., & Liu, J. (2019). The impact of cyber threats on data integrity and confidentiality. Computers & Security, 85, 212-224.
7. Sun, N., Li, T., Song, G., & Xia, H. (2021). Network security technology of intelligent information terminal based on mobile internet of things. Mobile Information Systems, 2021(1), 6676946
8. Cui, J., Chen, W., Wan, Q., Gan, Z., & Ning, Z. (2024). Design and Analysis of a Mobile Automation Testing Framework: Evidence and AI Enhancement from

Chinese Internet Technological Companies: A Case Study. Frontiers in Business, Economics and Management, 14(2), 163-170.
9. C. Horan and H. Saiedian, “Cyber crime investigation: Landscape, challenges, and future research directions,” J. Cybersecur. Priv., vol. 1, no. 4, pp. 580–596, 2021.
10. Cui, J., Liu, H., & Wan, Q. (2024). Measuring the Digital Assets, Brand Services and Service Quality Quantitative Analysis: Evidence from China. International Journal of Social Sciences and Public Administration, 2(3), 503-510.
11. Cui, J., Wan, Q., Wang, W., Hu, S., Gan, Z., & Ning, Z. (2024). Research on Alibaba company’s Digital Human Resource management and Recruitment Information Platform: A systematic case study. International Journal of Global Economics and Management, 2(3), 162 172.
12. 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).
13. Miller, G. 2020. "The intelligence coup of the century": For decades, the CIA read the encrypted communications of allies and adversaries. The Washington Post, February 11. Accessed December 20, 2023
14. Meserole, C. 2022. Digital authoritarianism and religious repression in China (Testimony before the Congressional Executive Commission on China. Hearing on "Control of Religion in China through Digital Authoritarianism).
15. S. O. Baror, H. S. Venter, and R. Adeyemi, “A natural human language framework for digital forensic readiness in the public cloud,” Australian J. Forensic Sci., vol. 53, no. 5, pp. 566–591, 2021.
16. T. Baker, P. Buck, F. Iqbal, and Q. Shi, “The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics,” Int. J. Digital Crime. Forensics (IJDCF), vol. 12, no. 1, pp. 1–13, 2020.
17. F. Delerue, “Reinterpretation or contestation of international law in cyberspace?” Isr. Law Rev., vol. 52, no. 3, pp. 295–326, 2019
18. O. Korzachenko and K. Cherniavskyi, “Applications: revolutionary changes in web development,” Modeling and Information Systems in Economics, no. 99, pp. 92–101, Nov. 2020,
19. W. Chen, H. Lu, M. Li, and Y. Sun, “Network protocol analysis base on WeChat PC version,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11635 LNCS, pp. 288–297, 2019
20. Layton, P. 2020. Artificial intelligence, big data and autonomous systems along the belt and road: Towards private security companies with Chinese characteristics? Small Wars & Insurgencies 31 (4):874–97.
21. Wang, B., Cui, J., & Mottan, K. (2024). Exploration and Analysis of Chinese University Students' Performance in Business Innovation. Economics & Management Information, 1-9