A Discussion Regarding The Function Of Computers In Online Criminal Investigation For Companies During Disasters And Cyber Crises: An Exhaustive Research

Peng Jinyin 1st , Divya Midhunchakkaravarthy 2nd

Cite this paper as: Peng Jinyin, Divya Midhunchakkaravarthy (2024) A Discussion Regarding The Function Of Computers In Online Criminal Investigation For Companies During Disasters And Cyber Crises: An Exhaustive Research". *Frontiers in Health Informatics,* (8), 5334-5342

ABSTRACT

When looking at technology-based evidence of wrongdoing, the area of digital forensics is crucial. Computers are now essential in digital forensics because of the massive and complicated nature of digital data. This article will explore the many ways computers have helped digital forensics, with a focus on evidence gathering, processing, and presentation. Improvements in computing power have made it easier for forensic investigators to gather, store, and evaluate digital evidence. Opportunities and difficulties have arisen for digital forensics professionals due to the proliferation of networked devices and developments in data storage and retrieval. Data recovery, forensic analysis tools, and machine learning are some of the computing technologies that this study emphasizes as crucial for improving the efficiency and precision of investigations. In addition, it delves into the ethical and legal aspects of digital forensics and the part computers play in this field. By clarifying the mutually advantageous link between computers and digital forensics, this study highlights the importance of multidisciplinary collaboration and continued technical improvements in combating cyber threats and guaranteeing the accuracy of digital investigations. The hypothesis that computers may have a place in digital forensics is the foundation of the research. In order to stay competitive in today's digital economy, all of these sectors are adopting digitization. As a result of digitization, corporate operations are now more faster and more efficient. All that is required to benefit from digitization is a technological device, such as a computer.

Keywords: *World Of Technology, Internet, Digital Investigation, Criminality.*

1. INTRODUCTION

Cybercrime has increased dramatically in this age of pervasive digital technology, calling for fresh approaches to investigation to keep up with the ever-changing internet. In the fight against cyber threats, the discipline of digital forensics—which entails gathering, analyzing, and preserving electronic evidence—has become increasingly important. Cybercrime relies on computers, which are also the foundation of forensic analysis, therefore these tools are crucial to the investigation. The use of complex computational algorithms is becoming more important for forensic professionals due to the exponential growth of digital footprints across various platforms and devices. In this paper, the researcher delve into the significance of computers in digital forensics and discover how they help with gathering, analyzing, and investigating evidence. The researcher delves into the relationship between technology and forensics, as a thorough grasp of computers is essential for unraveling the complex web of digital evidence. In order to seek justice and maintain digital integrity in an ever-changing digital universe, it is very necessary to grasp the dynamic interaction between computers and digital evidence. This century has seen a meteoric rise in the usage of the Internet and related technologies. There is no doubt that this development is associated with the worldwide increase in digital crimes, commonly referred to as e-crimes (AlKadi et al., 2019). The mitigation, proof of identity, investigation, and conviction of correlated crimes are being tested by these new digital crimes. Because cybercrime is so intricate, a new discipline of forensic science called computer forensics has developed in recent years. Computer forensics is an emerging field of study that seeks to identify cybercrimes and collect digital evidence for use in court by means of computational inquiry and analysis. A plethora of fascinating and difficult cryptography and computer security concerns have emerged as a direct outcome of this emerging discipline that combines expertise in IT, law, and forensics. More and more municipal police departments are showing interest in computer forensics. In almost every kind of enforcement activity, it has become an indispensable instrument for competent judges. There hasn't been enough investment to make it as accurate as alternatives, such as fingerprint analysis. Consequently, the true worth and reliability of digital evidence isn't always communicated to the judicial system. Examining legal procedures through the lens of scientific knowledge and cutting-edge technology is the domain of digital forensics. In order to discover what precisely occurred on a digital device, digital forensics seeks to give a thorough investigation and construct a recorded chain of proof and evidence (Aamir et al., 2021).

2. BACKGROUND OF THE STUDY

What exactly is presently referred to as digital forensics was more often referred to as "computer forensics" until the late 1990s. The field of computer forensics was first developed by law enforcement professionals with an interest in computers. In an effort to fortify cybersecurity, data localization, and sensitive safeguarding information, the National People's Congress formally approved the Chinese Cybersecurity Law. These measures are part of the researcher's plan to reduce "major risks" by the year 2026. Information security education and emergency exercises mimicking ransomware assaults are two examples of the steps taken. Their applications will reach more than 45,000 industrial businesses. The entry-level requirement for most cyber security positions is a bachelor's degree in computer science, IT, or a related discipline. The Chinese government is taking cybersecurity very seriously, and they are making it very clear that international enterprises operating in the country must adhere to Chinese law by merging VPN and data security legislation into a single cybersecurity act. Liability definitions and restrictions are also part of cybersecurity legislation. The idea of military-civil fusion is central to China's cybersecurity strategy; it promotes cooperation and the merging of governmental and commercial capabilities (Aassal et al., 2020).

3. PURPOSE OF THE RESEARCH

By upgrading their catastrophe recovery plans and processes, businesses may better respond to interruptions caused by cybercrime. The purpose of this qualitative Delphi research was just that. The individuals engaged in IT catastrophe recovery were the focus of a qualitative approach as the researcher developed a new strategy for responding. Finding patterns or similarities, the researcher surveyed 22 experts with a combined five-year background in five separate catastrophe recovery situations. Finding out how companies currently deal with IT disaster recovery and getting back to normal operations was the main goal of the inquiry. The researchers have developed a new model to help understand how IT disaster recovery operations may be affected by extra security measures or computer incident response frameworks. Instead of using a case study or any other qualitative research tool, the investigator opted for the Delphi method since the students' aims were learning about the factors that influence individual responses and how to improve the process of disaster response.

4. LITERATURE REVIEW

"The word deliberate method for maintaining, recognizing, collecting, comprehension, and preserving evidence relating to computer structures, including the relevant rules and regulations, procedures for ensuring the confidentiality of documentation, reporting the findings in a manner that is factual, and giving testimony from professionals with regards to the outcomes in a legal or administrative proceeding" (Yannick et al., 2021). Each of digital forensics' five subfields—computer, network, mobile device, memory, and email forensics—focuses on a specific kind of digital evidence. Data processing and storage, including its acquisition, preservation, retrieval, and presentation, is the domain of computer forensics, as stated by Alghamdi. Using scientifically defined techniques, digital evidence may be collected, aggregated, recognized, reviewed, and recorded from various digital sources that are actively processing and providing data. This process is called network forensics. The goal is to find out what happened during an illegal attempt to harm, compromise, or disrupt the system's components, or how to fix the system after an attack. Mobile device forensics is a subfield of digital forensics that focuses on the safe and reliable extraction of digital evidence from mobile devices according to predetermined standards (Haija & Zein-Sabatto, 2020).

5. RESEARCH QUESTION

- What role does presentation play in computer-based digital forensics?

6. 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.

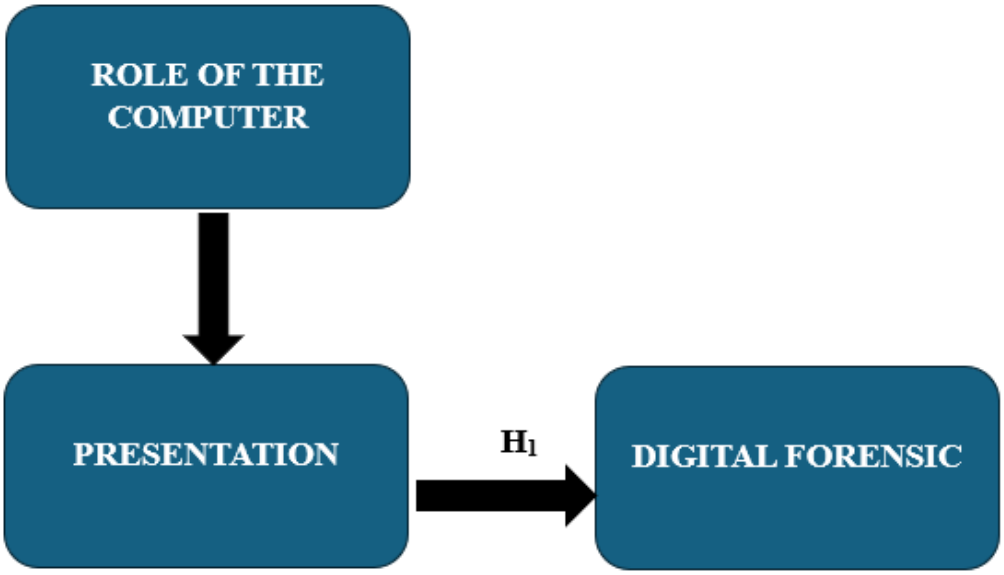
Sampling: After pilot research with 20 Chinese Researcher, 1100 Rao-soft pupils were included in the final Investors. Male and female Researcher were picked at random and then given a total of 1,455 surveys to fill out. A total of 1253 questionnaires were used for the calculation after 1300 were received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

Data and Measurement: 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.

7. CONCEPTUAL FRAMEWORK



8. RESULT

❖ Factor analysis

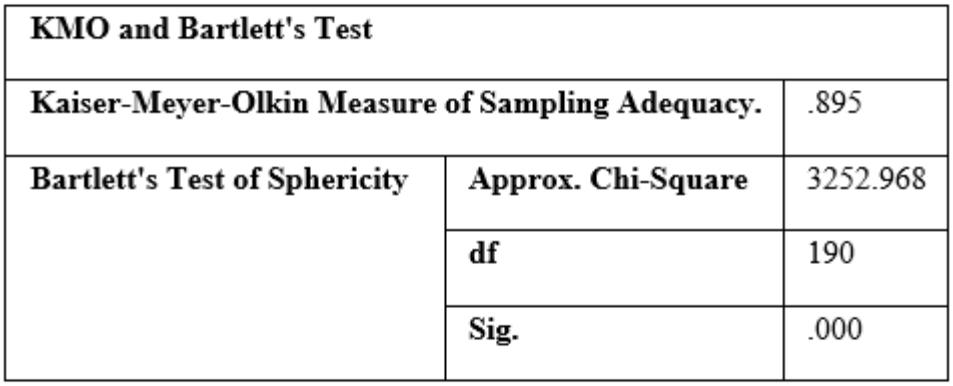
One typical use of Factor Analysis (FA) is to verify the existence of latent components in observable data. When there are not easily observable visual or diagnostic markers, it is common practice to utilize regression coefficients to produce ratings. In FA, models are essential for success. Finding 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: .895
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 0.895 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.		.895
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 0.895. Utilizing 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

Computers are now an integral part of researchers' daily lives, whether it's for personal tasks (like keeping track of finances) or professional ones (like making sales). A wide range of organizations and enterprises, from mom-and-pop shops to huge corporations, have sprung up to meet the growing need for computer-based services. The expansion of multimedia, electronic service networks, and other types of communication technology has also given companies more alternatives than ever before for doing business, exchanging money, and providing services. The capacity of computers to automate procedures is leading to a rise in the independence of businesses. There is no longer any need to engage human labor for any work since computers have made it possible to automate most of them. From the production of high-end autos to the purchase of tickets, everything is automated. It may be more effective to consolidate inventory rather to build physical facilities in each place, given that many firms now exclusively operate online. There is no need for a large workforce (Agarwal et al., 2021).

- **Factor**

Presentation

Presenting information to those in attendance is what a presentation is all about. Presentations are speeches, lectures, introductions, or demonstrations that aim to educate, convince, inspire, motivate, create goodwill, or introduce a new product or concept. Preparation, organization, event planning, writing, visual aid use, stress management, and question & answer sessions are common components of presentations. An successful presentation for organizational success includes the following elements: the presenter, the audience, the message, the response, and the technique of speech delivery. Accountants providing a comprehensive analysis of a company's finances or entrepreneurs presenting their business plan to investors are two examples of the many tertiary employment environments that make extensive use of presentations. The phrase may also refer to an offering or introduction that is formal or ritualized, like a debutante's presentation. Keynote addresses are another name for certain types of presentations. The use of audience participation in interactive presentations is also on the rise. The speaker and the listener engage in a conversation rather than a monologue. Some of the benefits of an interactive presentation include fostering a feeling of camaraderie among the audience and drawing in a larger audience's attention (Ahmad et al., 2020).

- **Dependent variable**

Digital Forensic

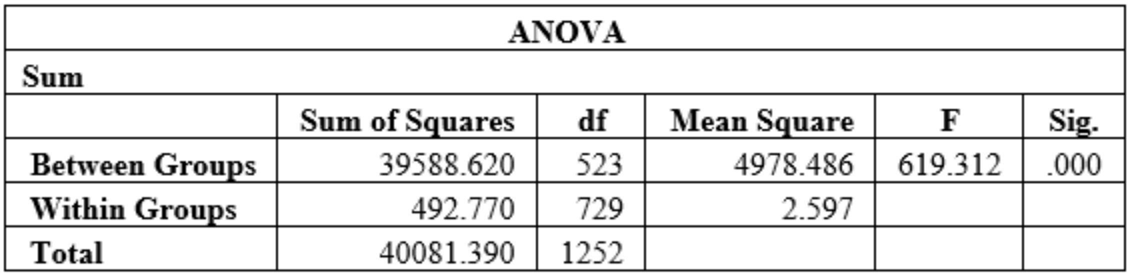
Forensic science includes the branch known as digital forensics. Cybercrime investigations, as well as civil and criminal cases, may benefit from its use. Both cybersecurity teams and law enforcement organizations use digital forensics to evaluate data obtained on suspect devices in murder investigations and identify malware attackers. One of the many uses for digital forensics is the standardization of evidence processing procedures for digital evidence. Similar to how police adhere to certain protocols when collecting physical evidence from a crime scene, investigators who focus on digital forensics adhere to a rigorous approach in order to prevent any kind of manipulation. In common use, "digital forensics" and "computer forensics" mean the same thing. In contrast to computer forensics, which mostly works with computing equipment like computers, tablets, smartphones, and other devices with central processing units (CPUs), digital forensics technically includes the collecting of evidence from any digital device. A relatively new field of cybersecurity known as digital forensics and incident response (DFIR) combines computer forensics with incident response operations to speed up the cleaning procedure after cyber-attacks while preserving any proof of related data (Mhiqani et al., 2020).

❖ Relationship between presentation and Digital Forensic

The team gets a chance to show off the ideas they came up with during the Presentation Phase, especially if they think those ideas are superior than the original one. During the Presentation Phase, decision-makers may ask the team questions and gauge the thoroughness of the study. The specific circumstances of forensic investigations need an individualized approach that makes full use of existing best practices. A formal written report outlining the discovery of pertinent information is a part of the digital analysis presentation. Getting the digital forensics evidence ready to submit to the court when the inquiry has concluded. It entails writing up the procedures and approaches used in the forensics investigation (Omari et al., 2021).

- ***H_{01} : There is no significant relationship between Presentation and Digital Forensic.***
- ***H_1: There is a significant relationship between Presentation and Digital Forensic.***

Table 2: H_1 ANOVA Test



ANOVA					
Sum					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	39588.620	523	4978.486	619.312	.000
Within Groups	492.770	729	2.597		
Total	40081.390	1252			

This investigation yields remarkable results. The F value is 619.312, achieving significance with a p-value of .000, which is below the .05 alpha threshold. This means ***"H_1: There is a significant relationship between Presentation and digital forensic."*** The alternative hypothesis is accepted, whereas the null hypothesis is rejected.

9. DISCUSSION

By surveying experts in IT disaster recovery and cybersecurity, this research addresses a knowledge vacuum in the existing literature. From this point forward, this trend will only worsen, say the experts. In spite of the fact that cybercrime poses new risks to businesses, conventional disaster recovery strategies still depend on data collected in the past for both catastrophe prevention and recovery. The transition from cybersecurity to disaster recovery may go more smoothly if the relevant parties work together. Cybersecurity training, whether general or specialized, may help with both preparation and the conceptual awareness required during disruptions caused by cybercrime. Disaster recovery responders and planners in the IT industry may find this valuable. Cybersecurity education has the potential to shed light on covert efforts to lessen danger. To assist companies get back up and running after disruptions to their operations, researchers are looking at methods to include more cybersecurity into the disaster recovery lifecycle.

10. CONCLUSION

In order to find ways to mitigate cybercrime's impact on disaster recovery, this study tapped into the domain expertise of cybersecurity professionals, local first responders, and academics. Respondents to the study emphasized the significance of incorporating cybersecurity issues into the disaster recovery process, even if the concept originated from applying emergency management concepts to natural catastrophes. The research indicates that in order for organizations to be better prepared, limit risks, learn from their mistakes, and raise responder awareness, cybersecurity expertise should be included into disaster recovery plans. More education on cybersecurity might lead to a more effective response to disaster recovery after a computer crime interruption. This study also aimed to determine if it would be possible to integrate cybersecurity frameworks with disaster recovery procedures. Integrating the incident response protocols, defensive measures, and monitoring included in popular cybersecurity frameworks into current IT disaster recovery plans and procedures is a simple and effective solution. Participants in this study often mentioned the benefits of merging the two ideas when asked about them. Businesses should look at ways to increase the cybersecurity expertise on their disaster recovery teams and include a cybersecurity framework in their disaster recovery plans, according to this study's results (Alazab et al., 2020).

REFFERENCE

M, Rizvi SSH, Hashmani MA, Zubair M, Ahmad J. Machine learning classification of port scanning and DDoS attacks: A comparative analysis. Mehran University Research Journal of Engineering and Technology. 2021;40(1):215–229.

Aassal A, El S, Baki A. Das, Verma RM. An in-depth benchmarking and evaluation of phishing detection research for security needs. IEEE Access. 2020;8:22170–22192.

Haija Q, Zein-Sabatto S. An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics. 2020;9(12):26

Agarwal A, Sharma P, Alshehri M, Mohamed AA, Alfarraj O. Classification model for accuracy and intrusion detection using machine learning approach. PeerJ Computer Science. 2021

Ahmad, I., and R.A. Alsemmeari. 2020. Towards improving the intrusion detection through ELM (extreme learning machine). *CMC Computers Materials & Continua* 65 (2): 1097–1111.

Mhiqani MN, Ahmad R, Abidin ZZ, Yassin W, Hassan A, Abdulkareem KH, Ali NS, Yunos Z. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences—Basel. 2020;10(15):41.

Omari M, Rawashdeh M, Qutaishat F, Alshira'H M, Ababneh N. An intelligent tree-based intrusion detection model for cyber security. Journal of Network and Systems Management. 2021;29(2):18

Alazab M, Alazab M, Shalaginov A, Mesleh A, Awajan A. Intelligent mobile malware detection using permission requests and API calls. Future Generation Computer Systems—the International Journal of eScience. 2020;107:509–521.

AlKadi O, Moustafa N, Turnbull B, Choo KKR. Mixture localization-based outliers models for securing data migration in cloud centers. IEEE Access. 2019;7:114607–114618.

Roland Yannick, Boumezoued Alexandre, Hillairet Caroline. Multivariate Hawkes process for cyber insurance. Annals of Actuarial Science. 2021;15(1):14–39.