Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 8
Open Access

A Consultation On The Role Of Computers In Online Criminal Investigation For Company During Disasters And Cyber Crises: A Thorough Analysis

Peng Jinyin 1st , Divya Midhunchakkaravarthy 2nd

Cite this paper as: Peng Jinyin, Divya Midhunchakkaravarthy (2024) A Consultation On The Role Of Computers In Online Criminal Investigation For Company During Disasters And Cyber Crises: A Thorough Analysis". *Frontiers in Health Informatics,* (8), 5280-5288

ABSTRACT

The field of digital forensics is vital for the investigation and analysis of digital evidence in the pursuit of criminal activity. Due to the ever-increasing amount and complexity of digital data, computers have become indispensable in digital forensics. Focusing on topics like evidence collection, processing, and presentation, the author of this piece will examine the many ways computers have aided digital forensics. Forensic investigators may now collect, store, and analyze digital evidence more effectively because to increases in processing power. The expansion of networked devices and advancements in data storage and retrieval have presented both opportunities and challenges for digital forensics experts. Computing technologies like as data recovery, forensic analysis software, and machine learning are highlighted in this paper as essential for enhancing the effectiveness and accuracy of investigations. Plus, it explores the role of computers in digital forensics as well as its legal and ethical dimensions. To combat cyber dangers and guarantee the veracity of digital investigations, this research emphasizes the need of interdisciplinary cooperation and ongoing technological advancements by elucidating the mutually beneficial relationship between computers and digital forensics. The study is based on the idea that computers may be useful in digital forensics. All of these industries are embracing digitalization as a way to run their businesses in an increasingly digital environment. The speed and efficiency of business processes have been substantially enhanced by digitalization. To take advantage of digitization, all the need is a computer or any other kind of technology.

Keywords: *Technological realm, online environment, forensics, cybercrime.*

1. INTRODUCTION

In this era of ubiquitous digital technology, cybercrime has skyrocketed, necessitating innovative methods of investigation to stay abreast with the dynamic nature of the internet. The field of digital forensics, which involves the collection, analysis, and preservation of electronic evidence, has grown in importance in the battle against cyber threats. As the medium for cybercrime and the bedrock of forensic analysis, computers play an essential role in this investigative expertise. As digital traces multiply across many devices and platforms, forensic experts must rely more and more on sophisticated computational methods. The importance of computers in digital forensics is explored in this paper, which sheds light on how computers facilitate evidence collection, analysis, and inquiry. An in-depth understanding of computers is crucial for understanding the intricate web of digital

evidence, and the researcher examines the interplay between technology and forensics. The ever-changing nature of the digital realm makes it all the more crucial to understand the dynamic interplay between computers and digital forensics in order to pursue justice and safeguard digital integrity. Internet and associated technology use has increased dramatically this century. Digital crimes, sometimes known as e-crimes, have been on the rise globally, and this trend is definitely linked to this expansion (Henderson et al., 2020). These digital crimes provide new challenges to linked crime prevention, identification, investigation, and conviction. Computer forensics is a relatively recent branch of forensic science that emerged in response to the exceedingly complicated nature of cybercrime. A relatively new academic discipline, computer forensics aims to use computational investigation and analysis to detect such crimes and gather digital evidence that may be used in legal proceedings. A multitude of intriguing and challenging cryptographic and computer security issues have surfaced as a result of this new field that brings together knowledge from the fields of law, forensics, and information technology. Computer forensics is attracting the attention of an increasing number of local law enforcement agencies. It has become an essential tool for judicial competence in almost all types of enforcement operations. It lags behind alternatives like fingerprint analysis because not enough money has been invested to make it as accurate. As a result, the truth about the value and dependability of digital evidence isn't always conveyed to the court system. The field of digital forensics uses scientific understanding and state-of-the-art technology to examine legal processes. In order to determine what exactly happened on a digital device, digital forensics attempts to provide a methodical investigation and arrange a documented chain of proof and evidence (Prade et al., 2020).

2. BACKGROUND OF THE STUDY

"Computer forensics" was the more common term for what is now known as digital forensics up until the late 1990s. Experts in law enforcement who had an interest in computers were the pioneers in computer forensics. The Chinese Cybersecurity Law, officially adopted by the National People's Congress, was reportedly passed to strengthen cybersecurity, data localization, and the protection of sensitive information. With these steps, the researcher want to mitigate "major risks" by 2026 (Hindy et al., 2020). Data security training and emergency drills simulating ransomware attacks are two of the measures used. Over 45,000 companies in the manufacturing industry will get their applications. The majority of cyber security professionals begin their employment with a bachelor's degree in computer science, information technology, or a closely related field. Through the consolidation of VPN and data security laws into a single cybersecurity statute, the Chinese government is increasing its oversight and making it plain that foreign companies must follow local regulations. Legislation pertaining to cybersecurity also includes regulations and definitions of liability. An important aspect of China's cyber policy is the concept of military-civil fusion, which encourages collaboration and the integration of resources between the military and the private sector (Kapoor et al., 2023).

3. PURPOSE OF THE RESEARCH

Businesses may improve their response to disruptions caused by cybercrime by revising their disaster

recovery procedures and policies. This qualitative Delphi study set out to do just that. We adopted a qualitative approach that centered on people involved in IT disaster recovery to build a new response strategy. To find commonalities or trends, the researcher polled 22 people with five years of expertise in five distinct disaster recovery scenarios. The crux of the investigation was to find out how businesses now handle IT catastrophe recovery and how they go back to regular operations. To better comprehend the potential effects of additional cybersecurity or computer incident response frameworks on IT disaster recovery operations, the researcher have devised a new model. Since the students' goals included understanding the elements that impact individual reactions and how to enhance the disaster response process, the researcher chose the Delphi method over a case study or other qualitative research strategy.

4. LITERATURE REVIEW

"The systematic approach to preserving, identifying, extracting, interpreting, and documenting evidence pertaining to computer systems, including applicable laws and regulations, procedures for ensuring the integrity of evidence, reporting the findings in a factual manner, and offering expert testimony in relation to the findings in a legal or administrative proceeding" (Rosso, 2020). Computer, network, mobile device, memory, and email forensics are the five branches of digital forensics, each of which deals with a different kind of digital evidence. Computer forensics, according to Alghamdi, is everything about data that has been processed and stored digitally, including how to get it, keep it, retrieve it, and display it. Digital evidence may be gathered, combined, identified, examined, corroborated, and recorded from a variety of digital sources that are actively processing and delivering data; this can be done using scientifically established procedures; this is known as network forensics. The objective is to learn how to restore the system after an assault or what occurred during an unauthorized effort to damage, compromise, or interrupt its components. As a branch of digital forensics, mobile device forensics seeks to reliably and securely extract digital evidence from mobile devices via the use of established protocols (Nordvik et al., 2019).

5. RESEARCH QUESTION

- How does the validation affect in digital forensics on computer?

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.

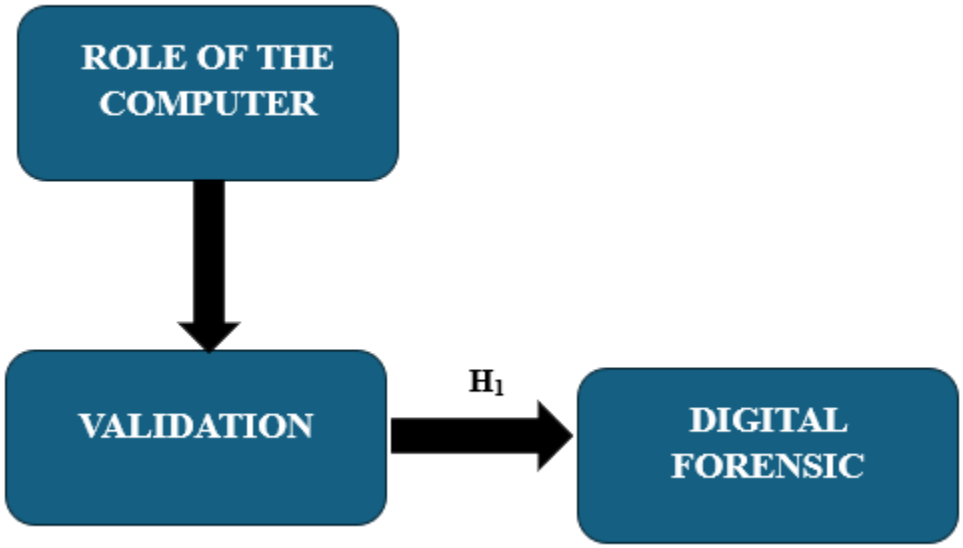
Sampling: After pilot research with 20 Chinese Researcher, 1100 Rao-soft pupils were included in the final Investors. Male and female Researcher were picked at random and then given a total of 1,455 surveys to fill out. A total of 1253 questionnaires were used for the calculation after 1300 were received 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: .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. 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 (Prade et al., 2019).

❖ **Factor**

Validation

It is critical to ensure that data from various sources and repositories will adhere to business standards and avoid corruption caused by type or context discrepancies while transferring and combining data. To avoid mistakes and data loss during a relocation, it is important to generate data that is consistent, accurate, and comprehensive. It is common practice in data warehousing to validate data before loading it into the ETL (Extraction, Transformation, and Load) system. To better understand the extent and kind of data conflicts, analysts conduct data validation tests. However, data inside a single program (like Microsoft Excel) or when combining basic data within a single data storage may also undergo data validation, since the word is generic and can be used to any sort of data (Mugisha & David, 2019).

❖ **Dependent variable**

Digital Forensic

Digital forensics is a subfield of forensic science. It is used to investigate cybercrimes and may also assist with civil and criminal investigations. Cybersecurity teams employ digital forensics to identify malware attackers, and law enforcement agencies utilize it to analyze data found on a suspect's devices in a homicide investigation. With digital evidence being handled similarly to conventional types of evidence, digital forensics has several applications. To avoid any kind of tampering, investigators who specialize in digital forensics follow a strict methodology, similar to how police follow certain rules while gathering physical evidence from a crime scene. The terms "digital forensics" and "computer forensics" are often used interchangeably. Digital forensics technically encompasses the collection of evidence from any digital device, as opposed to computer forensics, which primarily deals with computing devices like as computers, tablets, smartphones, and other devices having central processing units (CPUs). To expedite the cleanup process after cyber-attacks without compromising

any linked data evidence, a relatively new area of cybersecurity called digital forensics and incident response (DFIR) integrates computer forensics with incident response activities (Walter, 2020).

❖ **Relationship between Validation and Digital Forensic**

A data recovery strategy including goals, processes, and duties in the case of data loss should be in place before the student validate recovered data. Included in this plan should be a backup strategy that specifies the data to be backed up, how often, where, and for how long. A recovery time objective (RTO) that establishes the maximum acceptable length of downtime in hours or minutes and a recovery point objective (RPO) that defines the maximum acceptable amount of data loss in terms of time or transactions should also be included in the plan. A recovery process outlining the procedures to restore data from backup sources, including the responsibilities of the data recovery team, should also be included in the strategy. Lastly, make sure the recovered data is consistent, accurate, and full by implementing a testing and validation procedure.

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

Table 2: H_1 ANOVA Test

ANOVA					
Sum					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	39588.620	422	4978.486	619.312	.000
Within Groups	492.770	830	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 Validation and digital forensic."*** The alternative hypothesis is accepted, whereas the null hypothesis is rejected.

9. DISCUSSION

This study fills a gap in the literature by examining the consensus across professionals in the fields of cybersecurity and information technology disaster recovery. This tendency will, according to experts, only get worse from here on out. Despite the fact that cybercrime presents new threats to companies, traditional disaster recovery approaches continue to rely on historical data for both prevention and recovery from natural disasters. To ensure a smooth handoff from cybersecurity to catastrophe recovery, those in charge should collaborate. Preparedness for the planning phase and the conceptual awareness needed during an interruption caused by cybercrime may be enhanced by training in general or specialist cybersecurity measures. This can be useful for IT disaster recovery responders and planners. Unseen attempts to reduce risk may be illuminated by cybersecurity training. Researching

ways to include more cybersecurity into the disaster recovery lifecycle may help businesses recover from interruptions to their operations more quickly and efficiently.

10. CONCLUSION

This research relied on the knowledge and expertise of cybersecurity experts, first responders, and academics in the area to identify solutions to lessen the effect of cybercrime on disaster recovery efforts. Despite the idea's origins in emergency management principles applied to natural disasters, survey participants stressed the importance of including cybersecurity concerns into the disaster recovery process. Organizations should include cybersecurity knowledge into their disaster recovery plans, according to the study, so they may be better prepared, control risks, learn from their errors, and increase responder awareness. After a computer crime disruption, a better reaction to disaster recovery may be possible if more people were taught about cybersecurity. The feasibility of combining disaster recovery processes with cybersecurity frameworks was another focus of this research. A straightforward and efficient option is to include the incident response processes, defensive measures, and monitoring found in popular cybersecurity frameworks into preexisting IT disaster recovery plans and procedures. The advantages of combining the two concepts were often brought up by the participants in this research when questioned about them. This study's conclusions suggest that businesses should strengthen their disaster recovery plans by including a cybersecurity framework and investigate how to raise the level of cybersecurity knowledge on their disaster recovery teams (Stein & Jacobs, 2020).

REFFERENCE

Prade, P., Groβ, T., & Dewald, A. (2020). Forensic analysis of the resilient file system (ReFS) version 3.4. Forensic Science International: Digital Investigation, 32, 300915

Kapoor, N., Sulke, P., Pardeshi, P., Kakad, R., & Badiye, A. (2023). Introduction to Forensic Science. In Textbook of Forensic Science (pp. 41-66). Singapore: Springer Nature Singapore

Nordvik, R., Georges, H., Toolan, F., Axelsson, S., 2019. Reverse engineering of ReFS. Digit. Invest. 30, 127e147

Prade, P., Grob, T., Dewald, A., 2019. Forensic Analysis of the Resilient File System (ReFS) Version 3.4. Technical Report CS-2019-05. Department Informatik.

Mugisha, David. (2019). Role And Impact of Digital Forensics in Cyber Crime Investigations. International Journal of Cyber Criminology. 47. 3.

Walter, J., 2020. Threat Intel:Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic.

Stein, S., Jacobs, J., 2020. Cyber-attack hits U.S. health agency amid COVID-19 outbreak.

Rosso, K. D., 2020. New threat discovery shows commercial surveillanceware operators latest to exploit COVID-19

Hindy H., Brosset D., Bayne E., Seeam A., Tachtatzis C., Atkinson R., Bellekens X. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access. 2020;8:104650–104675.

Henderson, S., Roncone, G., Jones, S., Hultquist, J., Read, B., 2020. Vietnamese threat actors apt32 targeting Wuhan government and Chinese ministry of emergency management in latest example of COVID-19 related espionage.