Information Crimes and Investigation Challenge Combating Information Crimes: A Multidimensional Approach to Addressing Investigation Challenges in the Era of Digital Advancement

Prusha Qalandar Hussein

Law Department, University College of Goizha, Sulaymaniyah,Kurdistan Region -iraq

Email:prushaqalandar90@gmail.com

Key words:	Received:04/10/2024	ID No. 2762
Information crimes, Cybersecurity, Investigation challenges, Cybercrime, Digital Forensics	Accepted:23/11/2024	(PP 501 - 522)
	Published:30/11/2024	https://doi.org/10.21271/zjlp.22.sp.23

Abstract

In our increasingly digitized world, information crimes have emerged as a significant threat, encompassing a wide range of unlawful activities such as hacking, identity theft, and cyber espionage. This study explores the landscape of information crimes and the challenges faced by investigators in addressing and mitigating these offenses. The first aspect of this study examines the diverse realm of information crimes, providing an overview of the types of offenses that fall under this category. From financial fraud to data breaches, the spectrum of information crimes is vast, posing risks to individuals, businesses, and even nations. Understanding the nature and evolution of these crimes is crucial for developing effective investigation strategies and procedures. The second focus of this study is on the challenges faced by investigators when tackling information crimes. The dynamic and borderless nature of the digital realm presents unique obstacles, including issues related to jurisdiction, attribution, and the rapidly evolving tactics employed by cybercriminals.

Additionally, the study sheds light on the technological complexities that investigators face, such as encryption and anonymization tools that perpetrators exploit to conceal their activities. To address these challenges, the study suggests the implementation of multidimensional and collaborative approaches. International cooperation among law enforcement agencies, private sector entities, and cybersecurity experts is emphasized. The study also seeks continuous training and skill development for investigators to stay abreast of technological advancements. In conclusion, this paper tries to underscore the urgency of enhancing global efforts to combat information crimes. By comprehensively understanding the landscape of these offenses and addressing the specific challenges faced by investigators, we can better equip ourselves to safeguard the integrity of information in our interconnected world.

1. Introduction

To effectively counter information crimes, it is imperative to investigate the dynamics of the threat landscape. Cyber threats manifest in various forms, each posing unique challenges to cybersecurity and law enforcement efforts. The motives behind these crimes are diverse, ranging from financial gain and political agendas to ideological beliefs and state-sponsored activities (Rowlingston, R, 2007). One prevalent form of cybercrime is hacking, wherein individuals or groups exploit vulnerabilities in computer systems to gain unauthorized access. This can lead to the theft of sensitive information, disruption of services, or the compromise of critical infrastructure. Data breaches, another common threat, involve unauthorized access to databases, resulting in the exposure of personal or confidential information.

Identity theft is a persistent challenge, wherein cybercriminals manipulate or steal personal information for fraudulent activities. This not only harms individuals but also has severe repercussions for businesses and financial institutions. Cyber espionage, often orchestrated by nation-states, involves the theft of classified information for political or economic advantage. The evolution of ransomware presents a growing concern. Cybercriminals use malicious software to encrypt data, demanding a ransom for its release. This not only affects individuals but also poses a significant risk to organizations, disrupting operations and causing financial losses (Jones, R., & Brown, S., 2021).

The interconnectedness of systems and the proliferation of the Internet of Things (IoT) further amplify the threat landscape. As more devices become connected, the potential attack surface expands, providing cybercriminals with new avenues for exploitation. To address these challenges, a comprehensive understanding of the threat landscape is essential. Cybersecurity and law enforcement professionals must stay abreast of emerging trends, tactics, and techniques employed by cybercriminals. This requires continuous learning, collaboration, and the development of advanced tools and methodologies to stay one step ahead of evolving threats. In the next sections, we will explore the strategies and collaborative efforts required to effectively combat information crimes in this dynamic digital landscape.

2. Methodology

This paper will be relying on a descriptive method of the secondary collected data combining both qualitative and quantitative approaches to gather a comprehensive understanding of information crimes and the challenges encountered by investigators.

3. Ethical Considerations & Limitations

This paper will adhere to ethical guidelines, ensuring the confidentiality of participants and the responsible use of sensitive information. The study will prioritize the security and privacy of data, recognizing the sensitive nature of the subject matter. It is essential to acknowledge the limitations of the research, such as potential biases in available literature, the dynamic nature of cyber threats, and the challenges associated with obtaining accurate and up-to-date information. These limitations will be considered in the interpretation of results.

4. Literature Review

A thorough review of existing literature on cybercrime, cybersecurity, and law enforcement strategies will be conducted. This will provide insights into the historical context, evolving nature, and existing countermeasures against information crimes. The literature review will include academic publications, industry reports, and government documents.

5. The Research Aims

The research seeks to gain a comprehensive understanding of the landscape of information crimes. This involves delving into the various types of information crimes, their prevalence, and the methodologies employed by perpetrators. The research aims to identify and analyze the challenges encountered by investigators when dealing with information crimes. This could include obstacles related to technology, legal frameworks, or other aspects that hinder effective investigation and prosecution.

Based on the insights gained, the research aims to propose strategies for combating evolving threats related to information crimes. This may involve suggesting

technological solutions, legal reforms, or procedural improvements to enhance the overall effectiveness of combating information crimes.

The research acknowledges a gap in the existing literature, indicating a need for more comprehensive insights into information crimes, especially within the context of Iraq and the Kurdistan region. By filling this gap, the study contributes to the academic understanding of the subject and provides a foundation for future research. A practical aspect of the research is to contribute to the enhancement of the investigation system in Iraq and the Kurdistan Region. This involves proposing specific measures such as proper training for investigators and raising awareness about information crimes, potentially leading to more effective prevention and response mechanisms. Finally, the research aims to not only deepen the theoretical understanding of information crimes but also to have practical implications by suggesting strategies for improvement in the investigation systems of Iraq and the Kurdistan region. This dual focus on academic contribution and practical application is likely to make the research valuable for both the scholarly community and law enforcement practitioners.

6. The Hypotheses

The following hypotheses suggest critical aspects that need consideration in the realm of information crimes and cybersecurity. This is including;

1. The diversity and complexity of information crimes require multifaceted investigative approaches. Information crimes encompass a wide range of activities, each with unique characteristics and challenges. This hypothesis posits that a one-size-fits-all investigative approach may not be sufficient. Instead, a multifaceted strategy that adapts to the diverse nature of information crimes is necessary. This might involve a combination of technological expertise, legal understanding, and collaboration with various stakeholders.

2. Collaboration among international law enforcement agencies and private sectors is imperative for effectively combating information crimes. Information crimes often transcend national borders, requiring a collaborative and coordinated effort to address them effectively. This hypothesis emphasizes the importance of international cooperation between law enforcement agencies and private sectors to share information, resources, and expertise in combating cyber threats. A united front is seen as essential in countering the global nature of information crimes.

3. Continuous training and skill development are crucial for investigators to keep pace with technological advancements in cybercrimes. Given the rapid evolution of technology, cybercriminals constantly adapt and employ sophisticated methods. This hypothesis suggests that investigators need ongoing training and skill development to stay abreast of the latest technological advancements and cyber threats. This includes understanding new attack vectors, tools, and techniques employed by cybercriminals.

These hypotheses collectively underscore the dynamic and complex nature of information crimes, emphasizing the need for a holistic, collaborative, and continuously evolving approach in addressing the challenges posed by cyber threats. The research can test these hypotheses to validate their significance and contribute to the development of effective strategies in combating information crimes.

7. Research Questions

These research questions are well constructed to address key aspects of information crimes and cybersecurity. The questions are including:

1. What are the various types of information crimes, and how have they evolved in the digital age? This question aims to provide a comprehensive understanding of the landscape of information crimes. By identifying and categorizing the various types of information crimes, the research can shed light on the evolution of these crimes in the context of technological advancements. This question encourages an exploration of the dynamic nature of cyber threats over time.

2. What are the primary challenges encountered by investigators when addressing information crimes? This question explores the specific obstacles faced by investigators in their efforts to combat cyber threats. By identifying and analyzing these challenges, the research can contribute valuable insights into areas that require attention and improvement, guiding the development of effective countermeasures.

3. How can multidimensional approaches involve international cooperation and continuous training aid in combating information crimes? This question focuses on potential solutions. It explores the effectiveness of multidimensional approaches, emphasizing international cooperation and continuous training, in addressing information crimes. By investigating successful strategies and understanding the impact

of collaboration and ongoing skill development, the research can offer practical recommendations for improving the overall response to cyber threats.

Together, these research questions create a comprehensive framework for examining the nature, challenges, and potential solutions related to information crimes. They guide the research toward providing a nuanced understanding of the multifaceted aspects of cybersecurity and law enforcement in the digital age.

8. Discussion

8.1 Evolution of Information Crimes in the Digital Age

Addressing information crimes presents investigators with multifaceted challenges that demand a sophisticated and adaptable approach. These challenges underscore the importance of hypothesis 1, emphasizing the need for diverse investigative strategies. Understanding these obstacles is crucial for developing effective countermeasures and enhancing the capabilities of law enforcement and cybersecurity professionals. As technology evolves, cybercriminals increasingly leverage encryption and advanced tools to conceal their activities. The use of anonymization techniques and encryption poses significant challenges for investigators, limiting their ability to track and attribute cybercrimes accurately.

The transnational nature of information crimes complicates investigations. Perpetrators often operate across borders, necessitating international collaboration. Jurisdictional issues, differing legal frameworks, and challenges in extradition processes hinder seamless cooperation among law enforcement agencies globally.

Case studies demonstrate how cybercriminals influence evolving technologies, necessitating investigators to possess varied skill sets in digital forensics and emerging security measures. Therefore, addressing the first research question about the evolution of information crimes in the digital age is crucial to understanding how the internet generates new opportunities for cybercriminals. Cybercrime encompasses offenses conducted on the internet, where computers serve as either tools or direct targets.
Classifying these crimes into distinct categories remains challenging due to their evolving nature (Jahankhani and Al-Nemart,2011).

Comparable to real-world crimes like murder or theft, cybercrimes often lack clear separations. In cybercrime, the computer, and the individual behind it can both serve as victims, depending on the primary target. This simplifies considering the computer either as the target or the tool. For instance, hacking involves attacking computer information and resources, exhibiting overlapping characteristics that defy perfect classification systems. When individuals become the primary targets, the computer operates as a tool rather than the target (Symantec, 2013). These crimes often exploit human vulnerabilities, resulting in real-world manifestations with substantial psychological and intangible damage (Yar, 2006). Such offenses, akin to traditional scams and theft, existed long before technological advancements, but the tools available now extend the criminal's reach and complexity, making tracing and legal actions more challenging. In contrast, crimes targeting the computer itself demand technical expertise from a select group of perpetrators. These offenses, closely tied to the advent of computers, reveal society's unpreparedness in combating such crimes. Despite the prevalence of these cybercrimes globally, regions like Africa and Nigeria still lack adequate technical knowledge to adapt and perpetrate these offenses effectively (Gordon, 2006).

Wall (2005) compiled a matrix of cybercrimes showcasing the different levels of opportunity each crime enables. Table 1 in Wall's work illustrates the internet's impact on criminal opportunity and behavior, depicting three levels of impact on the Y-axis.

Firstly, the internet has broadened avenues for traditional criminal activities like phreaking, chipping, fraud, and stalking. While these crimes existed previously, the internet has facilitated their widespread occurrence, increasing their frequency and prevalence. Traditional criminal groups not only use the internet for communication but also for executing offenses like fraud and money laundering more efficiently and with lower risks.

Secondly, the internet's influence has introduced new opportunities for traditional crimes such as cracking/hacking, viruses, large-scale fraud, online sex trafficking, and hate speech. While hacking traditionally targeted Confidentiality, Integrity, and Availability (CIA), recent advances include parasitic computing, where criminals use distant networks to store illegal content like pornographic images or pirated software.

Indeed, the profound impact of the internet has spawned emerging forms of crime like spam, denial of service attacks, intellectual property infringement, and fraudulent activities in online auctions. These new avenues reflect the transformative influence of the internet on criminal behavior and opportunity.

More opportunities for traditional crime (e.g. through communications)	**Integrity-related (Harmful-Trespass) Phreaking chipping**	**computer – related (Acquisition theft/deception) Frauds Pyramid schemes**	**Content-related 1 (obscenity) Trading sexual materials**	**content -related 2 (violence) Stalking personal harassment**
New opportunities for traditional crime (e.g., organization across boundaries)	**cracking/hacking Viruses H Activism**	**Multiple large-scale fraud 419 scams, trade secret theft, ID theft**	**Online gender trade Cam Girl sites**	**General hate speech organized pedophile rings(child abuse)**
New opportunities for new types of crime	**spams (List construction and content) Denial of service, information, Parasitic computing**	**Intellectual property piracy online gambling e-auction scams small-impact bulk fraud**	**Cyber-sex Cyber-Pimping**	**Online grooming,organized bomb talk/drug talk targeted hate speech**

Table 1 The Matrix of cybercrime: level of opportunity by type of crime (Wall, 2005)

As for the impact of the internet on criminal behavior, the table shows on the X-axis that there are four types of crime: integrity-related (harmful trespass), computer-related (acquisition theft/deception), content-related (obscenity), and content-related (violence). As Wall (2005) argues, for each type of crime there are three levels of harm: least, middle, and most harmful. For example, within the integrity-related (harmful trespass) type, phreaking and chipping are the least harmful, whereas denial of service and information warfare are the most harmful.

Multidimensional approaches also involve proactive prevention strategies. This includes robust cybersecurity frameworks, threat intelligence sharing, and public awareness campaigns. Preventing information crimes before they occur is as crucial as responding to them, and a proactive stance is essential for mitigating risks effectively.

Finally, understanding the evolution of information crimes, the challenges faced by investigators, and the role of multidimensional approaches provides a holistic view of the complex landscape of cybersecurity.

As technology continues to advance, these insights can guide the development of effective strategies to combat cyber threats and protect individuals, businesses, and governments in the digital age.

8.2 Addressing Investigative Challenges in Information Crimes

The challenges faced by investigators in the realm of information crimes necessitate strategic responses to overcome these hurdles. These challenges align with Hypothesis 1, underscoring the necessity for diverse investigative approaches. Encryption tools employed by offenders obstruct evidence collection, attribution, and subsequent prosecution. Addressing these complexities requires specialized training and collaborative efforts to navigate legal and technological barriers effectively. Hence, the central query to address is: What are the primary challenges encountered by investigators when tackling information crimes? Investment in specialized training programs for investigators in cyber forensics is crucial. These programs should cover the latest advancements in technology, digital forensics methodologies, and legal considerations. Equipping investigators with the necessary skills enhances their ability to navigate hardware and software complexities.

The growth in individuals using networked digital devices has led to an increase in criminal activity that necessitates forensic examinations (Brown, 2015). The expertise in Cyber Forensics enables the retrieval of evidence from such devices. This collected evidence is crucial in legal proceedings to establish the crime and prosecute cybercriminals. Indeed, the role of Cyber Forensic investigators and analysts is critical in the process of addressing information crimes. The following are aspects of their responsibilities:

1. **Collection: This involves the application of forensic procedures to gather digital evidence in a way that adheres to established protocols. Proper collection is crucial to ensure the admissibility of the evidence in legal proceedings. Mishandling this process could compromise the integrity of the data.**
2. **Examination: After collection, forensic investigators systematically examine the gathered data using specialized tools and techniques. The goal is to analyze the content**

of digital devices while preserving the integrity of the evidence. This step ensures that the information is accurately and thoroughly examined without any alterations.

3. Analysis: Data analysis is a crucial phase where investigators evaluate the relevance of the information to the requirements of the investigation. This includes identifying patterns, connections, and any mitigating circumstances. Analysis plays a vital role in understanding the context of the digital evidence and its significance in the case.

4. Reporting: Reporting involves the documentation and presentation of the findings from the digital evidence. Investigators use suitable documentation and visualization techniques to create reports that can be understood by legal professionals, judges, and other stakeholders. Clear and comprehensive reporting is essential for the successful prosecution of cybercriminals.

The whole process of gathering forensic evidence encounters various challenges, broadly classified into four areas: device obstacle (hardware obstacles), software complexities, challenges in cloud forensics, legal barriers and human-related difficulties (Karie & Venter, 2015; Lindsey, 2006; Mohay, 2005).

8.2.1 Hardware obstacles

The challenges related to hardware obstacles in cyber forensic investigations highlight the impact of evolving technology on evidence collection and analysis. Studies have shown instances where suspects replace the hard disk in their devices before Cyber Forensic experts gain access (National Institute of Justice, 2002; Brown, 2015). In such cases, suspects operate write blockers to transfer data between the two hard disks. Consequently, analyzing the new hard disk forensically may not reveal crucial evidence. Furthermore, evidence obtained from the new hard disk might lack coherence and clarity (Brown, 2015; Spafford, 2006).

Additionally, data obtained from a reset device could compound the issue as a part of the backup data might have been restored during the reset process. Some mobile devices feature hard disks with built-in algorithms that automatically erase data. As the technology for retrieving data from unused or data-erased devices is still evolving, accessing such information might experience delays. Consequently, Cyber Forensic experts face significant challenges in recovering data deleted from devices (Spafford,

2006). Addressing these hardware-related challenges requires a combination of advanced forensic techniques, continuous research and development, and collaboration within the cyber forensic community. As technology evolves, so must the methods employed by investigators to ensure the effective and accurate retrieval of digital evidence.

8.2.2 Digital Software Complications

The current technological era has brought substantial shifts in forensic evidence collection. The adoption of Platform as a Service (PaaS) and Software as a Service (SaaS) has transformed computing structures. Modern operating systems feature detailed logs, requiring cyber forensic experts to gather comprehensive background information on application accessibility, usage details, and user-specific data. While accessibility issues arise from discrepancies between applications and operating systems (Spafford, 2006; Giordano & Maciag, 2002). For instance, modifications to file content might not be traceable without comparing file versions or modified timestamps. Determining the extent of manipulation remains challenging for Cyber Forensic experts (Brown,C, 2015).

Certain applications and system log data can serve as evidence, but understanding their utilization remains nascent, complicating effective use in forensic investigations (Giordano & Maciag, 2002). For example, systems like Windows 8 document accessed Wi-Fi networks and data transmission, which can aid in data theft or intrusion investigations. However, correlating this data with violation events requires further research. Several mobile messaging applications automatically erase shared data, posing retrieval challenges for Cyber Forensic experts.

Encryption in mobile devices, aimed at securing data during retrieval, complicates decryption, especially in cases involving encrypted storage or devices themselves (Giordano & Maciag, 2002). Not providing mobile device PINs and passwords could have legal ramifications in certain jurisdictions. For instance, in the UK, withholding passwords under Schedule 7 of the Terrorism Act could result in arrest (legislation.gov.uk, 2008; Mandhai, 2017).

Finally, the integration of new technologies poses numerous challenges for cyber forensic experts. Addressing these challenges requires continuous research and adaptation to stay ahead of the evolving technological landscape.

8.2.3 Cloud Forensic Difficulties

The difficulties faced in cloud forensic investigations, particularly in the context of the integration of cloud computing with smart mobile devices, present obstacles in forensic investigations due to its adaptability and expansive nature (Lopez, Moon, & Park, 2016). Retrieving data from these devices, accessible from diverse locations, poses a challenge for investigators, necessitating a balance between data retrieval and user privacy protection. Expertise in anti-forensic tools and practices becomes crucial for accurate forensic analysis (Spafford, 2006; Lopez, Moon, & Park, 2016). Expertise in anti-forensic tools and practices becomes crucial for accurate forensic analysis in the cloud computing environment. Cloud-based applications facilitate cross-device data access, making it challenging to identify the source of alterations in cases where multiple compromised devices modify applications. This complexity can potentially obscure evidence (Everard, 2008).

8.2.4 Legal complexities

Data protection and privacy regulations have undergone changes globally, reflecting the evolving landscape of technology and personal information handling (Nelson et al., 2010). Cyber laws across various jurisdictions often fail to adequately address the intricacies of gathering forensic evidence in the digital age. For instance, a suspect's device may contain pertinent personal information crucial for an investigation, yet accessing such private data might be construed as a breach of user privacy (Spafford, 2006). The trend of companies allowing employees to use personal devices for official communications poses multiple challenges in data collection.

Accessing a user's email via webmail and a smart mobile device, including downloading associated attachments, might be considered unauthorized access to personal data. In the current legal landscape, extracting specific information from user devices is noted as a significant challenge (Williams, 2012).The legal complexities surrounding data protection and privacy regulations pose challenges for forensic investigations. The conflict between the need for investigation and the protection of user privacy, coupled

with the widespread use of personal devices for official purposes, raises issues of unauthorized access and the extraction of specific information from user devices.

These challenges underscore the need for a careful balance between the requirements of forensic analysis and the protection of individual privacy rights within the legal frameworks of different jurisdictions.

9. Crime Scene Challenges

Gathering information about the crime scene, including layout and potential digital devices, is crucial. Estimating the number of individuals or devices involved helps in resource allocation. The role of digital devices in investigations can often be underestimated, emphasizing the need for comprehensive planning. Before visiting the crime scene, acquiring pre-search intelligence is needed. Understanding the scene's layout, estimating the number of individuals or devices involved, and pinpointing relevant digital information aids in organizing resources for data capture. Deciding whether to remove digital devices from the scene or capture data on-site for later analysis is pivotal (Staniforth, 2013). Preserving evidence at a crime scene is paramount but should never compromise personal safety. Once safety is ensured, the preservation process can commence. It's crucial to clear uninvolved individuals from interacting with any digital devices to prevent inadvertent data damage that could complicate or compromise the investigation. Recording the physical crime scene through various means (photos, videos, sketches) aids in later identification of device locations. Documentation assists in making inferences about digital data based on physical evidence. Considering the multitude of digital devices at a crime scene, seizing every item is impractical due to budget and time constraints.

Decision-making regarding device seizure considers investigation type, device ownership, and available intelligence. Collaboration among lead investigators and legal experts is crucial in this process. When seizing a device, it is important to assess whether it is powered on. If active, capturing live data and documenting running programs is necessary before powering it down. Shutting down servers or critical systems follows specific procedures to avoid compromising data integrity. Devices should be sealed in evidence bags with unique reference numbers for identification, ensuring chain of custody. Once the crime scene is secure, attention shifts to technical considerations for

seizing devices. This comprehensive approach aligns with best practices in digital forensics and emphasizes the need for a well-coordinated and thoughtful process to ensure the integrity of evidence while considering practical constraints.

9.1 Live and Online Data Capture

Live data capture is essential for critical servers to prevent business disruption. Abruptly shutting down a device can risk data loss, particularly when dealing with encrypted data that may be inaccessible without the correct password after shutdown. High-tech investigations aim for reproducible steps and results, but live data undergoes constant change, making full replication impossible. Documenting live analysis safeguards captured data by creating evidence hashes during collection, curbing volatility. Historically, tracing website access evidence relied on local machine temporary files. However, evolving internet coding necessitates direct webpage access or service provider requests. Detailed data capture from social networks, notably in cyberbullying investigations, is increasingly pivotal in high-tech probes. Live data's fluid nature poses challenges. Safeguarding captured data via evidence hashes during collection is crucial. Accessing evidence from evolving internet technologies demands direct webpage access or collaboration with service providers. Detailed social network data capture has become vital in high-tech investigations, particularly cyberbullying cases (Cerone & Shaikh, 2008). Investigations need to adapt to the evolving landscape of internet technologies, requiring updated methods for evidence collection, especially in online environments. The complexities and challenges associated with live and online data capture in high-tech investigations, emphasizing the need for adaptability and advanced methodologies to ensure the integrity of captured data.

9.2 Offline (dead) Data Capture

Offline (dead) data capture is a crucial aspect of digital forensics, allowing investigators to collect and preserve data from a device for analysis without altering the original information. Traditional data capture involves replicating data from a device, typically a hard drive, for later analysis. This process is fundamental in digital forensics to retrieve evidence and gain insights into a device's usage and activities (Cerone & Shaikh, 2008). A critical tool used to maintain forensic integrity by preventing any write (modification) requests to the original data during the capture process. Write-blockers, available in physical and software forms, safeguard diverse digital devices from

investigator alterations. Physical blockers directly connect to devices and analysis machines, while software-based blockers interrupt driver behavior in the operating system.

Finally, offline (dead) data capture, when done using write-blockers, is a meticulous process that ensures the preservation of original data for forensic analysis, maintaining the integrity and reliability of the evidence collected. Both physical and software-based write-blockers are employed to prevent any unintentional or intentional modifications to the data during the investigation.

10. Case Study: High-Tech Investigation in a Legal Firm

10.1 Background

A legal firm initiated a high-tech investigation in response to reports of customers being sold misleading legal documentation. Concerns over potential malicious data tampering prompted the legal firm to take swift action, implementing legal measures to secure the premises and prevent the removal of digital evidence(Staniforth, 2013). The investigation aimed to uncover the extent of the issue and gather evidence for legal actions.

10.2 Investigative Measures:

Legal measures were implemented without forewarning the organization under scrutiny to prevent potential data tampering. A mandate was enforced, restricting the removal of digital devices from the premises to mitigate potential revenue loss. Prior intelligence indicated about 20 staff working on-site simultaneously, detailing the building's access points, including vehicle routes.

There was insufficient time or information to pinpoint the specific digital devices present on the premises. Both legal and high-tech investigation teams arrived at the premises the subsequent day. The area was secured by relocating everyone away from digital devices to maintain the integrity of potential evidence. Detailed documentation, including digital recordings and sketches, cataloged each device present on-site .

Most devices, primarily computers and laptops, were found inactive and disconnected. One active server was identified during the investigation. The memory of the active server was captured to document ongoing processes and connections before the server

was shut down. Forensic data was collected from all on-site devices, a process that spanned over 12 hours. The collected data was secured in tamper-proof bags to ensure the preservation of its integrity during transportation to a laboratory.

In the laboratory, the collected data underwent thorough analysis by the high-tech investigation team. The investigation's context provided crucial keywords and file types used to sift through the data. The analysis revealed pertinent files, emails, and documents related to the misleading legal documentation. These findings empowered the legal team to progress with their legal actions against the organization.

10.3 Outcome

The high-tech investigation, coupled with legal measures, successfully uncovered evidence of misleading legal documentation practices. The detailed documentation and forensic analysis provided a solid foundation for legal actions. The findings allowed the legal team to proceed with confidence, armed with the information necessary to address the reported issues and potentially rectify any damage caused to the firm's reputation. This case study highlights the importance of a coordinated approach between legal and high-tech investigation teams to ensure the successful collection and analysis of digital evidence in a legally sound manner.

11. Enhancing Global Collaboration Through Continuous Training to Combat Information Crimes

The counter against information crimes demands a multifaceted strategy intertwining international collaboration and continuous training, supported by Hypothesis 3, highlighting the paramount role of ongoing training in empowering investigative units amidst the evolving cyber threat landscape. Ongoing training is crucial for investigative units to adapt to the evolving cyber threat landscape. Agencies that prioritize skill enhancement demonstrate increased adaptability and effectiveness in countering information crimes. Information crimes are transnational, requiring a global approach to law enforcement and potential cooperation beyond national borders. International initiatives, such as the European Convention on Cybercrime Budapest (2001), underscore information exchange, legislative development, and public awareness campaigns on cybercrimes. These conventions stress stringent penalties, witness and victim safeguards, and robust legislative frameworks to combat transnational

cybercrimes. Yet, the complexity of modern crime exceeds individual countries' capacities, especially in addressing cross-border cyber threats.

Collaborative legal assistance between countries becomes essential to investigate these crimes effectively. An international entity facilitating communication and information exchange across borders becomes imperative, particularly for crimes transcending national jurisdictions (Rowlingston,2007).

Cybersecurity awareness training is a powerful tool in reducing security incidents, such as phishing attacks, malware infections, and data breaches (Saikayasit,2012). Tailoring cybersecurity awareness training to remote work is essential for securing home networks and devices. Integrating cybersecurity training into a comprehensive security strategy, including technical measures, policies, and incident response plans, strengthens defenses against evolving cyber threats. Cultivating a culture of cybersecurity consciousness among employees enhances overall organizational resilience. Legislative reforms are necessary to address the escalating frequency and sophistication of cyber threats.

Existing legal frameworks may lag behind technological advancements, creating gaps that cybercriminals exploit. Prioritizing proactive measures and accommodating emerging technologies through adaptive legal frameworks is crucial to effectively combat evolving digital risks.

Finally, Legislative reforms are seen as vital in addressing emerging cyber threats by establishing adaptable policy frameworks that define cyber crimes comprehensively, enforce stringent penalties, promote international cooperation, and accommodate evolving technologies. Also, the interconnectedness of international collaboration, continuous training, and legislative reforms as essential components of a holistic strategy to combat information crimes in an increasingly complex and interconnected digital landscape.

12. Conclusion

In conclusion, this paper emphasizes the complex scene of information crimes and the difficult challenges faced by investigators in the digital age. The evolution of these crimes highlights the need for a holistic understanding and adaptive strategies. The

diverse challenges, including jurisdictional issues, attribution complexities, and rapid technological advancements, necessitate a collaborative and multidimensional approach. The study advocates for international cooperation among law enforcement agencies, private sectors, and cybersecurity experts as a crucial element in addressing information crimes effectively. Continuous training and skill development for investigators are emphasized to keep pace with evolving cyber threats. The dynamic nature of these offenses requires adaptability and innovation in investigative approaches.

This paper's methodology, combining descriptive analysis, case studies, and comparative analysis, contributes to a comprehensive understanding of information crimes. The hypotheses and research questions guide the exploration of multifaceted investigative approaches, collaboration, and training. The findings illuminate the evolution of information crimes and the challenges investigators face, offering insights into hardware and software obstacles, legal complexities, and cloud forensics challenges.

Through practical case studies, the paper emphasizes the importance of meticulous planning and digital forensics in investigations. The call for enhanced global collaboration is grounded in the recognition of the transnational nature of information crimes.

Legislative reforms and cybersecurity awareness training are deemed essential components of a proactive strategy.

In essence, the conclusion reiterates the urgency of proactive measures, continuous skill development, and robust cybersecurity frameworks to safeguard information integrity in our interconnected world. The collective efforts and innovative strategies advocated in this paper aim to empower investigators to stay ahead of cyber threats and navigate the complexities of the digital era effectively.

13. Recommendations:

Implementing the following recommendations will contribute to building a robust cybersecurity ecosystem in Iraq and the Kurdistan Region, enhancing the ability to prevent, investigate, and respond to information crimes effectively. It's crucial to foster collaboration among various stakeholders, leverage international support, and tailor strategies to the unique circumstances of the region.

-Enhance Cyber Security Infrastructure:
Allocate resources to develop secure networks, intrusion detection systems, and firewalls.

-Specialized Training for Law Enforcement:
Establish training programs for law enforcement in digital forensics, data analysis, and cybercrime investigation. Collaborate internationally for expertise and resources.

-Collective Response and Threat Intelligence Sharing:
Foster collaboration among government agencies, private sector, and technology companies to share threat intelligence and collectively respond to cyber threats.

-Legal Framework Strengthening:
Update and strengthen legislation to comprehensively address information crimes, aligning with international standards. Develop specific laws for cybercrimes like hacking, data breaches, and online fraud.

-Cross-Border Collaboration:
Collaborate with neighboring countries and international organizations to combat cross-border cyber threats. Participate in regional cybersecurity initiatives and forums for shared expertise and resources.

REFERENCES

- **Brown, C. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55-119.**
- **Brown, S. (2015). Digital Forensics: Digital Evidence in Criminal Investigations. CRC Press.**
- **Cerone, A. & Shaikh, S. A. (2008). Formal analysis of security in interactive systems. In M. Gupta & R. Sharman (Eds.), Handbook of Research on Social and Organizational Liabilities in Information Security. IGI-Global, pp. 415-432 (Chapter 25).**
- **Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from Council of Europe.**
- **Everard, P. (2008). NATO and cyber terrorism, Response to Cyber Terrorism. In Edited by Center of Excellence Defence Against Terrorism, Ankara, Turkey, pp. 118-126.**

- **Giordano, J., & Maciag, T. (2002). High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program. Butterworth-Heinemann.**
- **Gordon, S., & Ford, R. (2006). Information Security: Protecting the Global Enterprise. Prentice Hall.**
- **Jahankhani, H., & Al-Nemrat, A. (2011). Information Security Management: Concepts and Practice. CRC Press.**
- **Legislation.gov.uk. (2008). Terrorism Act 2000. Retrieved from legislation.gov.uk.**
- **Lopez, J., Moon, S., & Park, Y. (2016). "Cloud Forensic Science: A Survey and Research Directions." International Journal of Digital Crime and Forensics (IJDCF), 8(1), pp.57-74.**
- **Mandhai, S. (2017). "UK Man Charged Over Not Providing Password." Al Jazeera. Retrieved from Al Jazeera.**
- **Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to Computer Forensics and Investigations, fourth ed. Cengage Learning, Boston.**
- **Rowlingston, H. (2007). "Cyber Crime: The Challenge in Asia." In M. Nadesan (Ed.), Cyber Crime and Society (pp. 137-146). Sage Publications.**
- **Rowlingston, R. (2007). Towards a strategy for E-crime prevention. In ICGeS Global e Security, Proceedings of the 3rd Annual International Conference, London, England, 18-20 April 2007. ISBN 978-0-9550008-4-3.**
- **Saikayasit, R., Stedmon, A. W., Lawson, G., & Fussey, P. (2012). User requirements for security and counter-terrorism initiatives. In P. Vink (Ed.), Advances in Social and Organizational Factors. CRC Press, Boca Raton, FL, pp. 256-265.**
- **Staniforth, A. (2013). Blackstone's Counter-Terrorism Handbook, third ed. Oxford University Press, Oxford.**
- **Symantec. (2013). Intelligence Report: October 2013. Retrieved from http://www.symantec.com/connect/blogs/symantec-intelligence-report-october-2013 (accessed January 2024).**
- **Wall, D. (2005). "The Internet as a Conduit for Criminals." In T. Holt & B. Schell (Eds.), Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (pp. 17-38). IGI Global.**

- **Williams, J. (2012). ACPO Good Practice Guide for Digital Evidence. Retrieved from http://www.acpo.police.uk/documents/crime/2011/20110-cba-digital-evidence-v5.pdf (accessed 1-12-2024).**
- **Yar, M. (2006). Cybercrime and Society. Sage Publication Ltd, London.**

ئاڵنگارییەکانی بەردەم لێکۆڵینەوە بۆ بەرەنگاربوونەوەی تاوانە زانیاری و ئەلکترۆنی و دیجیتاڵیەکاندا،
پەیڕەوکردنی ڕێبازێکی فرە ڕەهەندی بۆ چارەسەرکردنی ئاستەنگەکانی لێکۆڵینەوە لە سەردەمی پێشکەوتنی دیجیتاڵیدا

پروشە قەلەندەر حسێن
بەشی یاسا، کۆلێژی زانکۆیی گۆیژە، سلێمانی، هەرێمی کوردستان - عێراق
ئیمێل: prushaqalandar90@gmail.com

پوختە

لەبەردەوامی بەرەوپێشچوونی جیهان بەرەو دنیایی دیجیتاڵی بوون، تاوانەکانی زانیاری و ئەلکترۆنی وەک هەڕەشەیەکی بەرچاو سەریان هەڵداوە، کە ئەمەش کۆمەڵێک چالاکیی نایاسایی لەخۆ دەگرێت لەوانە هاککردن و دزینی ناسنامە و سیخوڕی ئەلیکترۆنی ....هتد. ئەم توێژینەوەیە خوێندنەوەو شیکاری بۆ ئەم شیوازە نوێیانەی تاوانکاری دەکات (تاوانەکانی زانیاری و ئەلکترۆنی) هەروەها باس لەو ئاڵنگارییانە دەکات کە رووبەڕووی لێکۆڵەران دەبنەوە لە ڕێگریکردن و چارەسەرکردن و کەمکردنەوەی ئەم جۆرە تاوانانەدا. ڕوانگەی یەکەمی ئەم توێژینەوەیە هەوڵی ناساندن و بەدواداچوون دەکات بۆ ئەو لایەنە فرە رەهەندییانەی کە تاوانەکانی زانیاری لەخۆ دەگرێت. ئەمەش وا دەکات تێڕوانینێکی گشتی لەبارەی جۆرەکانی ئەو تاوانانەی کەلەم جوارچیوەیەدا بخاتەڕوو، هەر لە ساختەکاری داراییەوە تا پێشێلکردنی داتاکان، شیوازە جیاوازەزەکانی تاوانەکانی زانیاری ، کە دەبنە هۆی هەڕەشە و مەترسی لەسەر تاکەکان، بازرگانییەکان و تەنانەت گەلانی وولاتان. هەربۆیە لەم روانگەیەوە تێگەیشتن لە مێژوو و سروشت و پەرەسەندنی ئەم تاوانانە بۆ پەرەپێدانی ستراتیژ و ڕێکارە کاریگەرەکانی لێکۆڵینەوە زۆر گرنگە . لایەنی دووەمی ئەم توێژینەوەیە جەختکردنە لەسەر ئەو ئاڵنگارییانەی کە لێکۆڵەران لە کاتی بەرەنگاربوونەوەی تاوانەکانی زانیاری و ئەلکترۆنیدا ڕووبەڕوویان دەبێتەوە، چونکە سروشتی داینامیکی و بێ سنووری بواری دیجیتاڵی بەربەستی ناوازە دەهێنێتە پیش، لەوانە پرسەکانی پەیوەست بە دەسەڵاتی دادوەری، درککردن بە تاوانەکان و تاکتیکەکانی پەرەسەندنی خێرا کە لەلایەن تاوانبارانی ئەلیکترۆنیەوە بەکاردەهێنرێن.

سەرەڕای ئەوەش، توێژینەوەکە ڕۆشنایی دەخاتە سەر ئەو ئاڵۆزییە تەکنەلۆژیانەی کە لێکۆڵەران ڕووبەڕووی دەبنەوە، وەکو ئامرازەکانی کۆدکردن و بێناوکردن و بێناسنامەیی کە تاوانباران بۆ شاردنەوەی چالاکییەکانیان دەیقۆزنەوە. بۆ چارەسەرکردنی ئەم ئاڵنگارییانە، توێژینەوەکە پێشنیاری پەیڕەوکردنی ڕێبازە فرەڕەهەند و هاوبەشەکان دەکات. جەخت لەسەر هاوکاری نێودەوڵەتی لە نێوان دەزگاکانی جێبەجێکردنی یاسا و دامەزراوەکانی کەرتی تایبەت و پسپۆڕانی ئاسایشی ئەلیکترۆنی دەکرێتەوە. هەروەها توێژینەوەکە بەدوای ڕاهێنان و پەرەپێدانی کارامەیی بەردەوامدا دەگەڕێت بۆ لێکۆڵەران بۆ ئەوەی ئاگاداری پێشکەوتنە تەکنەلۆژییەکان بن. لە کۆتاییدا ئەم توێژینەوەیە هەوڵدەدات جەخت لەسەر بەخێرایی بەدەمەوەچوون و بەرزکردنەوەی هەوڵە جیهانییەکان دەکاتەوە بۆ بەرەنگاربوونەوەی تاوانەکانی زانیاری و ئەلکترۆنی.

ئەمەش لە ڕێگای تێگەیشتنێکی گشتگیر لە شێوازی ئەنجامدانی ئەم تاوانانە و چارەسەرکردنی ئەو ئاڵنگارییە تایبەتانەی کە لێکۆڵەران ڕووبەڕوویان دەبێتەوە، ئەمەش وا دەکات کە هەمووان بتوانن باشتر خۆیان ئامادەبکەن بۆ پاراستنی یەکپارچەیی زانیارییەکان لە جیهانی بەیەکەوە بەستراودا.

وشەی سەرەکی: تاوانەکانی زانیاری، ئاسایشی ئەلیکترۆنی، ئاڵنگارییەکانی لێکۆڵینەوە، تاوانی ئەلیکترۆنی، پزیشکی دادوەری دیجیتاڵی.

الجرائم المعلوماتية وتحديات التحقيق في مواجهة الجرائم المعلوماتية؛ نهج متعدد الأبعاد لمعالجة تحديات التحقيق في عصر التقدم الرقمي

پروشه قلندر حسين

قسم القانون، جامعه گويژه، السليمانية، اقليم كوردستان – العراق

البريد الالكتروني: prushaqalandar90@gmail.com

الملخص

في عالمنا المتزايد التكنولوجيا، ظهرت الجرائم المعلوماتية كتهديد كبير، تشمل مجموعة واسعة من الأنشطة غير القانونية مثل القرصنة الإلكترونية وسرقة الهوية والتجسس الإلكتروني. تستكشف هذه الدراسة مشهد الجرائم المعلوماتية والتحديات التي تواجهها الفرق التحقيقية في التعامل مع هذه الجرائم وتخفيف آثارها. تتناول الجانب الأول من هذه الدراسة مجال الجرائم المعلوماتية المتنوع، وتقدم نظرة عامة على أنواع الجرائم التي تندرج تحت هذا التصنيف. من الاحتيال المالي إلى اختراقات البيانات، تتنوع طيف الجرائم المعلوماتية بشكل كبير، مما يشكل مخاطر على الأفراد والشركات وحتى الدول. فهم طبيعة وتطور هذه الجرائم أمر بالغ الأهمية لتطوير استراتيجيات التحقيق والإجراءات الفعالة. تتمحور النقطة الثانية من هذه الدراسة حول التحديات التي تواجه الفرق التحقيقية عند التعامل مع الجرائم المعلوماتية. يقدم العالم الرقمي الديناميكي والغير محدود عقبات فريدة، بما في ذلك المشاكل المتعلقة بالاختصاص والتسلسل الزمني وتطور التكتيكات التي يستخدمها المجرمون الإلكترونيون بسرعة. بالإضافة إلى ذلك، تسلط الدراسة الضوء على التعقيدات التكنولوجية التي يواجهها المحققون، مثل أدوات التشفير والتجهيز المجهولة التي يستغلها الجناة لإخفاء أنشطتهم. لمعالجة هذه التحديات، تقترح الدراسة تنفيذ نهج متعدد الأبعاد والتعاوني. يُؤكد التعاون الدولي بين وكالات إنفاذ القانون والقطاع الخاص وخبراء أمن المعلومات. تسعى الدراسة أيضًا إلى التدريب المستمر وتطوير المهارات للمحققين لمواكبة التطورات التكنولوجية. في الختام، تحاول هذه الورقة التأكيد على ضرورة تعزيز الجهود العالمية لمكافحة الجرائم المعلوماتية. من خلال فهم شامل لمشهد هذه الجرائم ومعالجة التحديات الخاصة التي تواجهها الفرق التحقيقية، يمكننا تجهيز أنفسنا بشكل أفضل لحماية نزاهة المعلومات في عالمنا المتصل.

الكلمات المفتاحية: الجرائم المعلوماتية، أمن المعلومات، تحديات التحقيق، جرائم الإنترنت، الفحص الرقمي.