Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATING COMPUTER FORENSICS FOR CYBERCRIME INVESTIGATIONS IN CRITICAL INFRASTRUCTURE SECTORS

VALERII BOZHYK[1], MYROSLAV POPOVYCH[2], OLHA KHAKHUTSIAK[3], MYKOLA DENYSENKO[4], OLEKSADR HERASYMENKO[5]

[1]Associate Professor, PhD in Law, Interregional Academy of Personnel Management, Ukraine
[2]Assistant, Doctor of Philosophy, Department of Criminal Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine
[3]Associate Professor, PhD in Law, Department of Criminal Justice at the Primary Scientific Institute of Law and Psychology, National Academy of Internal Affairs, Ukraine
[4]Director of the institute of State Security, PhD in Law, National Academy of the Security Service of Ukraine
[5]Doctoral student, PhD in Law, Department of Postgraduate and Doctoral Studies, National Academy of the Security Service of Ukraine
E-mail: [1]phd.lin.lin12@gmail.com, [2]popovych_MV@chnu.edu.ua, [3]olga_XX7@ukr.net, [4]denysenkomykola98@ukr.net, [5]herasym_olexandr@gmail.com

ABSTRACT

The increased digitization of critical infrastructure has compounded the threat of cybercrime in entrepreneurial enterprises handling high-value assets and sensitive information. Despite the abundance of literature on digital forensics, the unique application and value of these methods in critical infrastructure investigations remain largely unexplored. This study bridges this gap by evaluating the real-world efficacy of computer forensic techniques to detect and investigate crime in large industries, including finance, retail, and technology. A mixed-methods approach combined digital forensic analysis, statistical modeling, and expert interviews with 50 real-world cases. The findings reveal high rates of success in the use of forensic tools in uncovering evidence within complex business crimes, with data recovery and statistical analysis being most effective. Different from past studies, this research integrates empirical evidence and expert insights in assessing the real challenges and contributions of digital forensics in practice. This study contributes to the literature by developing a sectoral forensic framework, ascertaining legal and procedural limitations, and proposing paths for the uptake of AI-driven tools within forensic activities. These findings have practical implications in improving investigative accuracy, resource allocation, and interagency collaboration in cybercrime law enforcement.

Keywords: *Computer Forensics, Critical Infrastructure Security, Digital Evidence Analysis, Cybercrime In Entrepreneurship, Forensic Investigation Methods, AI In Digital Forensics, Statistical Forensic Evaluation.*

1. INTRODUCTION

In the era of pervasive digitalization, critical infrastructure complexes — whether financial, commercial, or technological — depend more and more on sophisticated information technologies. With this progress comes increased operational efficiency, though at the cost of increased vulnerability to hitherto unimaginable cyber attacks [1]. Crime against such infrastructures, and particularly entrepreneurial activities, poses actual threats to economic stability, national security, and public safety [2]. These crimes are often followed by complex cybercrime conspiracies, including data breaches, embezzlement, financial fraud, and unauthorized intrusions into computer systems, which require advanced technical methods of identification and investigation.

While digital forensics has emerged as a valuable tool in cybercrime investigations, the literature mainly addresses general cyber incidents, rather than the forensic challenges posed by critical infrastructure environments [3]. Moreover,

empirical research on a large scale, evaluating the performance of forensic techniques in industries and jurisdictions, is scarce. Forensic examination of business crime is also hampered by legal ambiguity regarding the admissibility, processing, and procedural use of digital evidence [4]. The inherent complexity of enterprise computer systems, combined with custom-built technology and run within varied regulatory regimes, requires a tailored forensic approach. This study fills this gap by systematically evaluating the effectiveness of computer forensic techniques in criminal investigations of crimes in entrepreneurial activities of critical infrastructure facilities. It employs a mixed-method approach that integrates forensic analysis, expert interviews, and statistical modeling from 50 case studies. The scope of this paper is limited to crimes against digital systems in three high-risk sectors — finance, retail, and technology — within critical infrastructure environments [5].

This study aims to evaluate the effectiveness of computer forensics in investigating criminal offenses within the entrepreneurial activities of critical infrastructure facilities. It seeks to identify methodological gaps, propose improvements, and explore the potential for integrating artificial intelligence to enhance forensic capabilities. The implementation of data analysis into these processes provides more possibilities for the effective identification of corrupt acts [6]. The main contributions of this research are three. First, it is an empirical assessment of the practical applicability of digital forensic methods, identifying which of the methods have the most significant impact. Second, it is a discussion of the procedural and legal challenges encountered by forensic investigations and suggests solutions to overcome these obstacles. Third, it explores the potential of integrating artificial intelligence and predictive analytics into digital forensic processes for increasing efficiency and accuracy.

To achieve this purpose, the study sets the following tasks:

1. To analyse modern computer forensic methods applicable to crimes in critical infrastructure, entrepreneurial activities.
2. To evaluate procedural and legal challenges in handling digital evidence within this context.
3. To investigate the role of interdisciplinary collaboration in improving forensic accuracy and legal outcomes.

The study has key practical implications. The findings can be utilized by law enforcers, forensic examiners, and corporate information security staff to optimize investigative procedures, redirect resources, and design targeted training initiatives. In addition, the study underpins the development of policy propositions for improving the legal and operational context encompassing digital forensics in business crime investigations.

2. LITERATURE REVIEW

The role of computer forensics in combating cybercrime has been extensively examined in recent years. However, most existing studies adopt a generalized approach, often overlooking the distinct challenges faced when investigating crimes within critical infrastructure facilities and entrepreneurial activities. This literature review critically evaluates prior works to identify theoretical and methodological gaps that the current study addresses. The source [2] emphasized the indispensable role of digital forensics in uncovering "invisible evidence" in cybercrime investigations, highlighting its relevance in the digital age. While their work provides foundational insight into the forensic process, it does not consider the nuanced application of these techniques in complex corporate systems or critical infrastructure sectors. Similarly, the study [3] discussed the importance of law enforcement in the EU and Ukraine in combating cybercrime, advocating for international cooperation. However, the focus remained on institutional roles rather than on the specific forensic tools and their effectiveness in enterprise-level investigations. The researchers [6] explored the benefits of digitalization in anti-crisis management for business entities. Their findings underscore the importance of data integrity and information security in mitigating corporate risks. Nevertheless, their work does not bridge this insight with the forensic methodologies necessary for post-crisis criminal investigations. Similarly, the researchers [5] demonstrated the utility of digital monitoring systems in detecting judicial corruption. Although relevant, their scope is limited to anti-corruption frameworks, with no evaluation of forensic tools used in broader business crime contexts [7]. The authors focused on digital evidence management in cybercrime investigations. While their recommendations are valuable for improving chain-of-custody protocols, the study did not differentiate between general cybercrime and corporate offenses, such as fraud or embezzlement within critical infrastructure [8]. The reference [9] provided a general overview of digital forensic tools, yet failed to address their practical

application in enterprise investigations. New research shows identified modern strategies used by cybercriminals to defraud corporations lack a forensic framework for detecting and countering such schemes [10]. Emerging studies have highlighted the promise of artificial intelligence and predictive analytics in enhancing cybercrime detection. The authors [11] developed models for predicting electronic fraud, demonstrating statistical effectiveness. However, their study did not integrate these models within forensic workflows or validate them in real investigative scenarios. Similarly, the authors [9] proposed a multivariate regression model to predict criminal behavior, contributing to the discourse on proactive crime prevention. Still, their findings lack applicability to the reactive nature of forensic investigations post-incident.

The cumulative review of literature reveals three key gaps. First, there is a lack of empirical research focusing specifically on the application of digital forensic methods in critical infrastructure and entrepreneurial contexts. Second, the effectiveness of forensic tools has not been comparatively assessed across sectors using real case data. Third, the potential synergy between AI-driven analytics and traditional forensic techniques remains underexplored.

Therefore, this study contributes uniquely by bridging these gaps. It focuses on empirical evidence from 50 documented cases, evaluates forensic tool effectiveness in real-world scenarios, and provides insights into integrating predictive technologies into forensic practice. By aligning technological innovation with legal investigation processes, the research seeks to enhance both procedural accuracy and judicial outcomes in cybercrime cases related to critical infrastructure.

3. METHODS

3.1. Study Design and Procedure

A mixed-method research design, which combines quantitative and qualitative approaches, was applied in this study to quantify the effectiveness of digital forensic tools in investigating criminal offenses against entrepreneurial activities in critical infrastructure facilities. The study was conducted in three phases (Figure 1):

1. Adequate forensic methods and case selection inclusion requirements were established after initial screening of digital crime cases according to corporate infrastructure. Inclusion requirements were focused on confirmed digital crimes, i.e., fraud, data breaches, or unauthorized access.

2. Fifty cases were selected from leading industries (finance, retail, and technology) through purposive sampling. All cases had established digital crime activity and were obtained from investigative reports of global law enforcement agencies and cybersecurity groups.

3. The forensic techniques applied in these cases were analyzed through statistical models, supplemented by qualitative interviews with digital forensic experts and law enforcement officials.

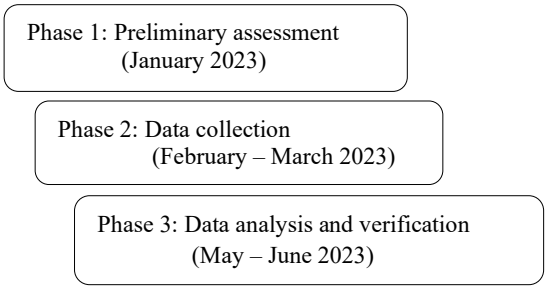

Figure 1: Phases of the Study
Source: Built by authors on [12].

3.2. Sample Structure and Criteria

The sample comprised 50 criminal cases of computer-based crimes where law enforcement authorities, cybersecurity centers, and compliance units of corporations carried out digital forensic investigations. The selection of cases was conducted based on the following criteria:

— Involvement of confirmed computer-based crimes;

— Presence of investigation data (digital artifacts, logs, forensic reports);

— Representation of industries (finance, retail, technology). The global and multi-sectoral composition offered variation in case history and investigation techniques (Table 1), which facilitated the generalizability of outcomes.

Table 1: Sample formation

Group of participants	Number of participants	Criteria for inclusion in the sample	Authorised bodies
Forensic analysts	20	Minimum 3 years of experience in digital forensics or investigations related to it	Federal Bureau of Investigation (USA); Europol, European Cybercrime Centre (EU); Nation Cyber Security Centre, Action Fraud (Great Britain); Royal Canadian Mounted Police, Canadian Centre for Cyber Security (Canada); Australian Cyber Security Centre, Australian Federal Police (Australia); Cyber Security Agency of Singapore, Singapore Police Force (Singapore); Ministry of Public Security, Cybersecurity Centre (China); Cyber Crime Police Stations, Indian Computer Emergency Response Team (India); Interpol and United Nations Office on Drugs and Crime, related to computer crimes in the business field
Employees of law enforcement agencies	20	Participation in at least two investigations of offences, related to entrepreneurial activity for the last five years	
IT-security specialist	10	Experience in digital security management and participation in judicial processes after incidents.	
Total	50	Balances representation of different sectors and geographical regions	

Source: developed by the author with the use of [13]–[17].

Participants offering expert opinions were:

— 20 experienced forensic professionals with a minimum of 3 years of experience;

— 20 police detectives who have taken part in a minimum of two relevant investigations in the past 5 years;

— 10 IT security specialists with experience in digital risk management and experience in legal proceedings.

3.3. Data Collection and Analysis Methods

Several tools and analysis methods were employed to evaluate forensic effectiveness:

1. Forensic Digital Analysis — All the cases were examined using forensic software for following digital traces, event reconstruction, and extracting deleted or hidden data. Methods included:

— Disk imaging (preservation of data integrity);

— File recovery (restoration of deleted or encrypted data).

— Log analysis (monitoring user activities);

2. Quantitative Effectiveness Assessment — Forensic case success was measured quantitatively using a standardized effectiveness index (Equation 1), comparing successful prosecutions to the overall number of cases using each forensic method.

$$Effectiveness\ index = \frac{Total\ number\ of\ events}{Number\ of\ successful\ forensic\ interventions} \times 100 \quad (1)$$

3. Qualitative Analysis: Semi-structured interviews were conducted with chosen experts (Annex A) to elicit procedural challenges, perceived effectiveness of procedures, and resource constraints.

4. Statistical Tools: SPSS was used for correlation and regression analysis to determine the effect of forensic interventions on successful prosecutions. HashCalc was used to verify data using hash checking. Additional tools were EnCase, FTK Imager, Wireshark, X-Ways Forensics, and SQL for querying data.

3.4. Rationale for Evaluation Criteria

Forensic effectiveness evaluation criteria were selected based on three dimensions:

— Technical Efficacy (rate of data recovery, traceability of logs);

— Legal Impact (court proceedings use);

— Practical Utility (expert satisfaction and resource feasibility).

The selected criteria are related to the operational goals of digital forensics—data integrity, evidence reliability, and admissibility to court.

3.5. Threats to Validity and Mitigation Strategies

Several potential threats to results validity were considered:

— Selection Bias: Addressed by incorporating varied cases from various countries and industries;

— Measurement Bias: Reduced by using standardized forensic effectiveness measures and cross-verifying results through expert triangulation;

— Temporal Validity: Protected by making sure all the cases were selected from investigations conducted within the last five years, guaranteeing contextual relevance.

— Interpretive Bias: Managed through expert interviews and peer review of coding plans during qualitative analysis.

This methodological precision guarantees the validity, reliability, and reproducibility of the research findings.

4. RESULTS

The study's analysis of 50 cases involving criminal activities in critical infrastructure facilities revealed that computer forensic methodologies played a pivotal role in resolving complex investigations. The results indicate that forensic techniques significantly enhance the detection and successful prosecution of crimes related to financial fraud, data theft, and unauthorized access.

4.1. Sectoral Distribution and Case Characteristics

The findings show a 71% overall effectiveness rate, with data recovery and statistical analysis being the most effective techniques. In particular, these methods were crucial for identifying breaches and reconstructing criminal activities. Image acquisition, while less effective compared to other methods, remained essential for preserving the integrity of digital evidence. Figure 2 presents a circular diagram of case allocation among business sectors.

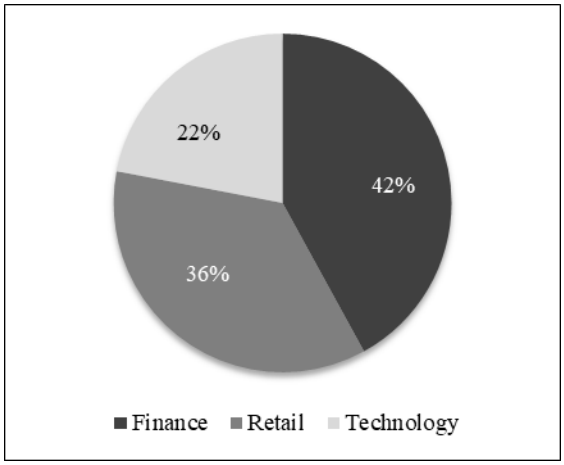

Figure 2: Case allocation by sectors.
Source: construed by the author using [18]

The financial sector demonstrates the highest level of cyber crimes, 21 cases were registered (42% of the total number). This indicates the vulnerability of financial institutions due to confidential data nature or large volumes of monetary transactions. The main threats include data leakage, fraud, and insider trading. 18 cases were registered in retail trades (36%). This relates to both online and offline businesses, emphasising the difficulties of protecting customers' data and transactions. The main threats are fraud with credit cards and clients' data leakage. The technological sector accounts for 11 cases (22%), which reflect attacks on digital infrastructure, in particular, hacking, intellectual property theft, and attacks on software and hardware. Rapid technological development complicates cybersecurity. The wide increase of cyber crimes in financial and retail sectors demonstrates the need for enhancing cybersecurity through personnel training, enhancing data protection protocols, and effective response measures. Enhancing regulatory supervision and policies is necessary to protect financial and customer information. Legislation should also be updated with consideration of new threats in the digital sphere. The effectiveness of different forensic methods used in the process of investigation was evaluated using the effectiveness index, which was calculated as follows:

$$Effectiveness\ index = \left(\frac{50}{35}\right) \times 100 = 142{,}86\% \quad (2)$$

Achieved an effectiveness index of 142,86 indicates that forensic interventions were, on average, successful in solving a significant number of cases of the studied ones. Exceeding 100%, the effectiveness index demonstrates that forensic methods were not only effective but, probably, contributed to numerous successful solutions in a lower number of situations. A high percentage indicates the significant influence of forensic methods on investigation and solving computer crimes in the business environment. This can improve the trust of law enforcement agencies as well as companies in forensic analysis. Conclusions can influence the allocation of resources on forensic technologies and education by organisations. Considering the demonstrated success, organisations can consider the possibility of increasing investments in digital forensics for further results improvement. These findings are consistent with trends noted by [1] and [9], who reported heightened cyber threats in sectors with high-value digital assets. However, unlike prior works, this study offers a forensic-centered

analysis, highlighting investigative challenges and methodological outcomes across each sector.

4.2. Forensic Method Effectiveness

The overall effectiveness index for digital forensic interventions across the cases was calculated at 142.86%, indicating multiple successful outcomes per intervention in several instances. The success rates of individual methods are presented in Figure 3.

Data Recovery: Used in 45 cases, with 32 successful applications (71.1% effectiveness). This method was particularly useful in restoring deleted transaction records and identifying altered system logs.

— Statistical Analysis: Employed in 35 cases, contributing to 25 successful outcomes (71.4%). It enabled pattern recognition and correlation of events to specific actors.

— Log Analysis: Applied in 40 cases with a 70% success rate. This method was critical in reconstructing digital timelines and tracing unauthorized access.

— Image Acquisition: Used in all 50 cases but had a lower effectiveness rate (60%). While essential for data integrity, this technique often requires complementary methods to support prosecution.

Figure 3 highlights that forensic techniques with analytical depth (statistical and log analysis) outperformed purely technical methods in investigative impact. These results support the findings of Delgado et al. [22], who emphasized the synergistic effect of integrating forensic intelligence with investigative analysis.

4.3. Correlation Between Forensic Interventions and Legal Success

Figure 4 illustrates a strong positive correlation ($r \approx 0.82$) between the number of forensic interventions and the success of legal prosecutions. This relationship confirms that the strategic application of forensic tools increases the probability of successful case resolution. The regression model suggests that each additional forensic intervention increases the likelihood of prosecutorial success, supporting similar observations by Wüllenweber & Giles [20].

4.4. Temporal Trends

Chronological analysis of computer crime cases for the last five years indicates the growing tendency in reports on such offences and their successful prosecution. Table 2 presents an annual distribution of cases and their results, and demonstrates stable growth of both registered cases and successful legal prosecutions. This growth is especially noticeable after the introduction of improved forensic expertise tools.

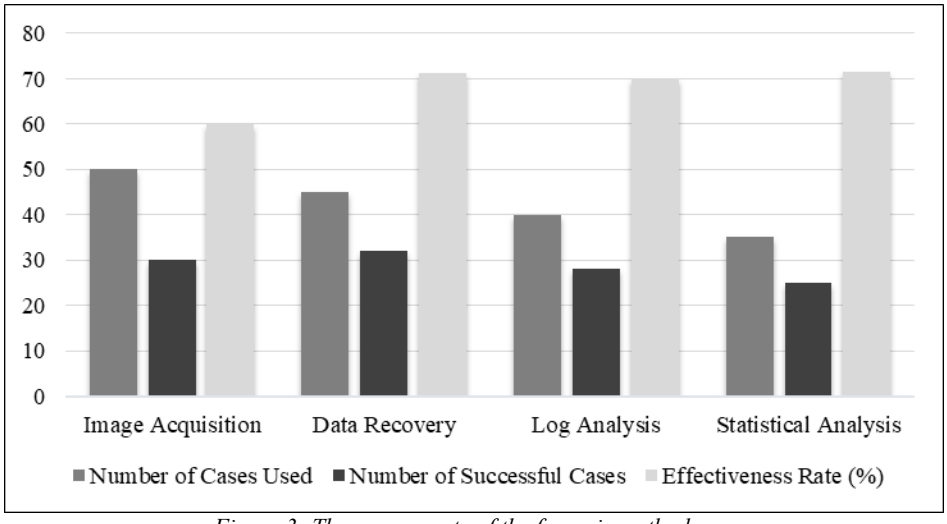

Figure 3: The success rate of the forensic method use.
Source: construes by the author with the use of [19], [20].

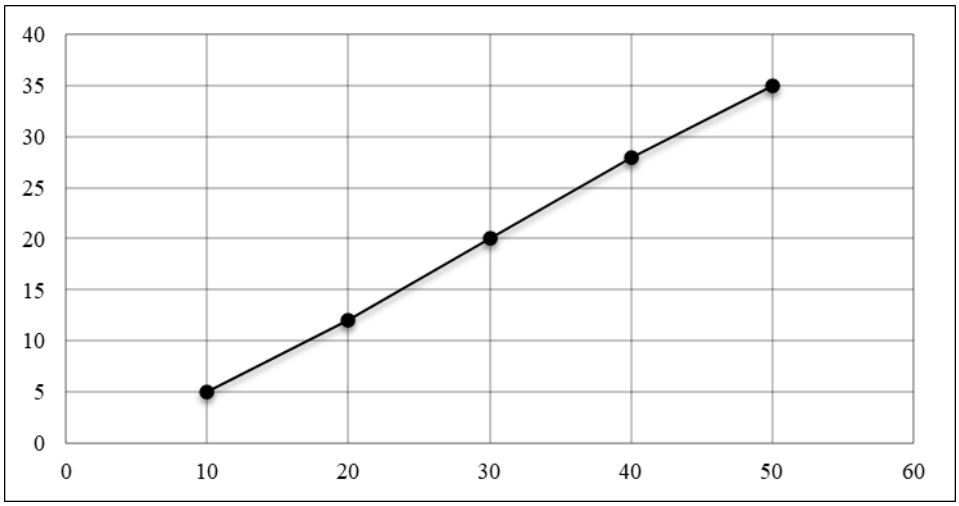

Figure 4: Correlation between forensic interventions and successful legal prosecution
Source: construed by the author using [21], [22].

Table 2 demonstrates changes in computer crime investigation in business within the last five years. The growth of the number of reported events and successful legal cases before the year 2022 indicates an improvement in the possibilities of forensic expertise and law enforcement agencies. At the same time, the reduction in 2023 underlines the challenges investigators face due to the complex strategies cyber offenders use. Data in Table 2 show that despite the contribution of digital forensics in the increase of successful prosecutions, constant investments in training, resources, and technologies are essential for the further growth of these indicators. These findings highlight the need for sustained investment in forensic technologies and specialized training programs to maintain investigative capabilities within critical infrastructure environments.

Table 2: Chronological tendencies in case-solving

Year	Reported cases	Successful legal prosecutions
2019	5	3
2020	8	5
2021	12	8
2022	15	12
2023	10	7

Source: construed by the author using [23], [24].

4.5. Expert Insights and Qualitative Findings

Interviews with forensic analysts and investigators revealed three major themes:

1. Data Complexity: 68% of respondents cited the growing volume and complexity of digital data as a primary obstacle to efficient analysis.

2. Training Needs: 62% emphasized the importance of continuous education in emerging forensic technologies.

3. Resource Allocation: 54% identified insufficient resources as a limitation in conducting comprehensive investigations.

These qualitative insights suggest that while technological tools are improving, human and organizational capacity remains a bottleneck in maximizing forensic effectiveness.

4.6. Strengths and Weaknesses of the Study

Strengths:

— Cross-sector analysis of real-world cases ensures high applicability of findings.

— Quantitative and qualitative triangulation enhances result validity.

— Clear identification of the most effective forensic tools.

Weaknesses:

— Limited to three industrial sectors and may not generalize to all critical infrastructure domains.

— Potential regional bias, as most case data were derived from Europe and North America.

— Technological changes may reduce the relevance of current findings over time.

Despite these limitations, the study presents a comprehensive evaluation of computer forensic effectiveness and offers strategic insights for policy and practice.

5. DISCUSSION

The results of this study confirm the central role of computer forensics in supporting the discovery, investigation, and prosecution of cyber-

enabled crimes in strategic infrastructure entrepreneurial activities. The results verify the hypothesis that advanced forensic methods, when systematically applied, significantly improve investigative outcomes in advanced digital media.

5.1. Interpretation of Findings

The high success rates of data recovery, statistical analysis, and log analysis are indicators of the operational effectiveness of computer forensics. These techniques offered verifiable evidence that not only assisted legal proceedings but also explained the chain of digital events surrounding the offenses. The 71 %+ effectiveness rate of core methods is an indicator of the practical utility of combining technical tools with analytical strategies.

The positive high correlation ($r \approx 0.82$) between forensic intervention frequency and successful legal cases further supports the assumption that forensics is not only contributory but rather a central part of modern criminal investigation in digital settings. This supports the need for proactive forensic application throughout the complete investigation process.

5.2. Comparison with Prior Research

The results are partly in alignment with the evidence put forward by authors [2], but they emphasized the authority of digital technology against cybercrime without going beyond common law enforcement practices. In contrast to the research of authors [1], based on the conceptual application of digital forensic principles, in this research, method-specific effectiveness was shown in practice-based corporate crime cases.

Furthermore, although the authors [3] explored the use of digitalization for business resilience, they never emphasized post-crisis forensic investigations. This study continues the line of reasoning by demonstrating how forensic technology is capable of solving crises, particularly in sectors involving sensitive financial and operational data.

Studies such as [6] and [7] brought digital solutions to highlight corruption detection and evidence management, respectively. But their inability to tackle the effectiveness of some forensic methods in business settings indicates the novelty of the present study. Moreover, this study is distinct from predictive-model-based studies like authors [10] because it addresses retrospective forensic effectiveness rather than proactive risk forecasting. Nevertheless, the findings suggest a potential synergy between AI-based prediction and forensic analysis, an area noted for future research.

5.3. Contributions to the Field

This research offers several new contributions to the digital forensics and cybercrime investigation field:

— It offers a comprehensive, sector-specific evaluation of forensic methods in 50 documented cases, with empirical performance standards;

— It uncovers invaluable methodological deficiencies and legal barriers in managing digital evidence in critical infrastructure contexts;

— It presents a forensic-performance model that can inform investigation protocols and resource planning strategies

— It provides new opportunities for the incorporation of AI-driven predictive tools into digital forensic workflows.

These contributions not only contribute to scholarly knowledge in digital forensics in practical contexts but also offer operational guidance for law enforcement, cybersecurity specialists, and legal professionals.

5.4. Limitations and Implications

Despite the robust methodology, there are some limitations to be considered. The research focused on the three industries — finance, retail, and technology — and might therefore have limited the scope of its applicability to other sectors of critical infrastructure, such as energy or transport. Additionally, although the sample case was global, it primarily relied on experience from European and North American agencies and might therefore not reflect cybercrime investigations in less developed jurisdictions.

Technological obsolescence also constitutes a drawback. Since modes of cybercrime evolve extremely fast, the effectiveness of existing forensic methodologies could get lost unless renovated frequently by innovations and training.

5.5. Directions for Future Research

Future studies need to pursue the following avenues:

1. Broadening coverage of sectors towards research into neglected areas such as public health and utilities;

2. Incorporation of longitudinal data to track the altering effectiveness of forensic methods over time;

3. Exploring the application of artificial intelligence, machine learning, and predictive analytics to forensic processes;

4. Evaluating digital forensics in emerging legal environments, such as cross-border data sovereignty and cloud-enabled evidence gathering.

5.6. Limitations

While this study offers valuable insights into the effectiveness of computer forensics in investigating cyber-enabled crimes in critical infrastructure, several limitations must be acknowledged:

— Sectoral Scope: The research focused exclusively on the finance, retail, and technology sectors. While these are among the most vulnerable to digital threats, findings may not generalize to other critical domains such as healthcare, energy, or transportation.

— Geographical Concentration: The case data were predominantly sourced from agencies in Europe, North America, and the Asia-Pacific regions with advanced cybercrime units. Thus, the outcomes may not accurately reflect contexts where digital forensic capabilities are less mature or underfunded.

— Technological Obsolescence: Given the rapidly evolving nature of cybercrime and digital tools, some forensic methods evaluated in this study may lose relevance as new attack vectors emerge and forensic technologies evolve.

— Retrospective Bias: The study employed a retrospective analysis of previously closed cases. This may exclude dynamic or ongoing investigative practices and limit the study's ability to capture evolving forensic decision-making in real time.

— Expert Interview Bias: Qualitative data were based on self-reported experiences of forensic practitioners and law enforcement officers. Despite careful triangulation, subjective bias cannot be entirely ruled out.

5.7. Recommendations

In light of these limitations and based on the findings, several recommendations are proposed for both practitioners and researchers:

— Expand Sectoral Analysis: Future investigations should include additional infrastructure sectors (e.g., utilities, healthcare, transportation) to build a more comprehensive understanding of forensic applicability across domains.

— Invest in Training and Capacity Building: Law enforcement and forensic analysts should undergo continuous training to adapt to new digital tools and cybercrime tactics. Tailored modules focused on infrastructure-specific forensic challenges are especially needed.

— Develop Cross-Jurisdictional Protocols: To address variability in legal and technical standards across countries, international frameworks for digital evidence handling should be developed and harmonized.

— Integrate Predictive Analytics with Forensics: Future research should explore the fusion of predictive models and forensic methods to enable both proactive detection and reactive investigation of cyber-enabled offenses.

— Standardize Forensic Effectiveness Metrics: Developing universally accepted indices for measuring forensic impact will allow better benchmarking across jurisdictions and cases.

— Invest in AI-Driven Forensic Tools: Policy and research funding should support the design and validation of artificial intelligence systems capable of automating parts of digital evidence acquisition, classification, and interpretation.

6. CONCLUSIONS

The current study has facilitated a comprehensive and empirically validated assessment of the utility of computer forensic techniques in criminal investigations involving entrepreneurial activities related to entrepreneurial activities in strategic infrastructure industries. With its examination of 50 recorded cases from finance, retail, and technology industries, the study has confirmed the practical utility of integrating digital forensic tools into modern investigative frameworks.

The most significant results are that forensic techniques, particularly data recovery, statistical analysis, and log analysis, greatly increase the likelihood of successful legal outcomes. The established 71 %+ effectiveness rate of primary techniques confirms the operational efficiency of these tools in extracting, storing, and analysing digital evidence. The satisfactory correlation between the number of forensic interventions and legal success also supports the strategic significance of digital forensics in complex corporate crime cases.

As opposed to previous research that was either sector non-specific or conceptually based, this study contributes in new ways by:

— Providing sector-specific empirical examination based on real case data.

— Providing method-specific evaluation of forensic effectiveness.

— Highlighting practical and procedural concerns facing practitioners.

— Proposing a blueprint for integrating artificial intelligence with forensic processes.

The consequences of the findings are far-reaching as applied. Forensic procedures can be enhanced, resources optimally distributed, and training programs optimized by law enforcement authorities, cybersecurity professionals, and judicial institutions, utilizing the findings. Corporate actors in key infrastructure industries can also utilize these findings to enhance internal investigative capacities and minimize exposure to cyberattacks.

This study also opens up new doors for additional research. Introducing AI and machine learning in forensic procedures, codifying efficacy measures, and expanding sectoral and geographical range are critical milestones toward advancing the discipline. By addressing these sectors, future studies can further enhance the flexibility, precision, and international applicability of digital forensic science.

Lastly, this research vindicates the place of computer forensics as the backbone of cybercrime investigation and business risk management. In the era of growing digital threats, the ability to identify properly, examine, and prosecute technology-enabled crimes is not only a technical necessity but a strategic imperative for national defense and economic well-being.

REFERENCES:

[1] L. Klasén, N. Fock, and R. Forchheimer, "The invisible evidence: Digital forensics as key to solving crimes in the digital age", *Forensic Science International*, Vol. 362, 2024, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

[2] I. Kopotun, A. Nikitin, N. Dombrovan, V. Tulinov, and D. Kyslenko, "Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU", *TEM Journal*, Vol. 9, Issue 2, 2020, pp. 460-468. https://doi.org/10.18421/tem92-06

[3] D. Kabachenko, O. Korolenko, N. Kutova, O. Churikanova, and R. Shchokin, "Implementation of Digitization for Anti-Crisis Management of Business Entities", *Economic Affairs*, Vol. 68, No. 1s, 2023, pp. 361-369. https://doi.org/10.46852/0424-2513.1s.2023.39

[4] A. Slonopas, "What is digital forensics? A closer examination of the field. American Public University" [online] *American Public University*, 2024. [Accessed 27 December 2024]. Available from: https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/

[5] O. S. Oliinyk, R. M. Shestopalov, V. O. Zarosylo, M. I. Stankovic, and S. G. Golubitsky, "Economic Security Through Criminal Policies", *Revista Científica General José María Córdova*, Vol. 20, No. 38, 2022, pp. 265-285. https://doi.org/10.21830/19006586.899

[6] V. Maziychuk, A. Voightko, Y. Tymoshenko, V., Tsikalo, and S. Syrovatka, "The Effectiveness of Electronic Declaration Monitoring in the Detection and Investigation of Corruption Offenses in the Judicial System", *Pakistan Journal of Life and Social Sciences (PJLSS)*, Vol. 22, No. 2, 2024, pp. 4833-4845. https://doi.org/10.57239/pjlss-2024-22.2.00358

[7] M. Morina, F. Azemi, M. A. Eren, I. Zejneli, and E. Papajorgji, "Crime Scene in Cybercrime Criminal Offenses: Evidence Management and Processing", *Academic Journal of Interdisciplinary Studies*, Vol. 12, No. 2, 2023, pp. 179-194. https://doi.org/10.36941/ajis-2023-0041

[8] M. S. Rana, M. M. Hasan, and M. Moneruzzaman, "An Introduction to Digital Forensics (Cyber Forensics)", *International Journal of Research Publication and Reviews*, Vol. 4, No. 12, 2023, pp. 1769-1771. https://doi.org/10.55248/gengpi.4.1223.123427

[9] S. Metts, and M. S. Bressler, "From Fraudsters to Scammers and Cyber Villains, Tech-Savvy Criminals are Out to Steal Your Money", *Journal of Accounting and Finance*, Vol. 23, No. 4, 2023, pp. 92-105. https://doi.org/10.33423/jaf.v23i4.6450

[10] O. Alabi, and A. David, "Model for Forecasting Electronic Fraud Threats on Selected Electronic Payment Channels Using Linear Regression", *International Journal of Information Technology*, Vol. 14, No. 5, 2022, pp. 2657-2666. https://doi.org/10.1007/s41870-022-00939-4

[11] S. Shukla, P. K. Jain, C. R. Babu, and R. Pamula, "A Multivariate Regression Model for Identifying, Analyzing and Predicting Crimes", *Wireless Personal Communications*, Vol. 113, No. 4, 2020, pp. 2447-2461. https://doi.org/10.1007/s11277-020-07335-w

[12] Data analysis, statistical & process improvement tools [online] *Minitab*, 2024. [Accessed 27 December 2024]. Available from:https://www.minitab.com/en-us/

[13] SurveyMonkey [online] [Accessed 27 December 2024]. Available from: https://www.surveymonkey.com/

[14] United Nations Office on Drugs and Crime [online] [Accessed 27 December 2024]. Available from: https://www.unodc.org/

[15] INTERPOL [online] [Accessed 27 December 2024]. Available from: https://www.interpol.int/

[16] Singapore Police Force (SPF) [online] [Accessed 27 December 2024]. Available from: https://www.police.gov.sg/

[17] Bundeskriminalamt. Areas of crime [online] [Accessed 27 December 2024]. Available from: https://www.bka.de/EN/OurTasks/AreasOfCrime/areasofcrime_node.html

[18] IBM SPSS Statistics [online] *IBM*, 2024. [Accessed 27 December 2024]. Available from: https://www.ibm.com/products/spss-statistics

[19] OpenText, encase forensic [online] *OpenText*, 2024. [Accessed 27 December 2024]. Available from: https://www.opentext.com/products/encase-forensic

[20] S. Wüllenweber, and S. Giles, "The Effectiveness of Forensic Evidence in the Investigation of Volume Crime Scenes", *Science & Justice*, Vol. 61, Issue 5, 2021, pp. 542-554. https://doi.org/10.1016/j.scijus.2021.06.008

[21] Correlation analysis. [online] *QuestionPro*, 2024. [Accessed 27 December 2024]. Available from: https://www.questionpro.com/features/correlation-analysis.html

[22] Y. Delgado, B. S. Price, P. J. Speaker, and S. L. Stoiloff, "Forensic Intelligence: Data Analytics as the Bridge Between Forensic Science and Investigation", *Forensic Science International Synergy*, Vol. 3, 2021, 100162. https://doi.org/10.1016/j.fsisyn.2021.100162

[23] SQL query for MySQL [online] *SQL Manager*, 2024. [Accessed 27 December 2024]. Available from: https://www.sqlmanager.net/products/mysql/query

[24] Forensic Science Strategic Research Plan 2022-2026 (Report NCJ 304856). [online] *National Institute of Justice*, 2022. [Accessed 27 December 2024]. Available from: https://www.ojp.gov/pdffiles1/nij/304856.pdf

Annex A

Questionnaire for the interview

Target audience:

The questionnaire is assigned for the survey of forensics experts, employees of law enforcement agencies and investigators, experienced in the use of digital forensics for investigation of criminal offences in entrepreneurial activity.

Information about the interviewee:

- Name:
- Position/rank:
- Organisation:
- Experience in forensics (years):

Section 1: Background information

1. Could you please briefly describe your work experience with digital forensics in business investigations? [Open-ended response]
2. What criminal offences related to entrepreneurial activity did you see in your work? [Open-ended response]

Section 2: Forensic tools and methods

1. Which digital forensics tool do you usually use in investigations?
   - EnCase
   - Thermal Imaging Camera FTK
   - X1 Social Discovery
   - Other (please indicate): _____
2. Which tools were the most effective in data and evidence recovery, based on your experience? Why? [Open-ended response]
3. What specific methods do you use in digital evidence analysis? [Open-ended response]

Section 3: Case outcomes and effectiveness

1. Could you please tell about a situation, when digital expertise significantly affected the outcomes? What role did forensic analysis play? [Open-ended response]
2. How do you evaluate the effectiveness of digital forensics compared to traditional investigation methods in commercial crimes? [Open-ended response]
3. Did you face any problems while using digital forensics in investigations? If yes, explain [Open-ended response]

Section 4: Future ideas

1. What features of digital forensics, do you believe, improve the investigation of business-related crimes in the future the most? [Open-ended response]
2. What would you recommend improving digital forensics integration in business crimes investigation? [Open-ended response]
3. Would you like to say something more about the role of digital forensics in the investigation of criminal offences in entrepreneurial activity? [Open-ended response]

Instructions to interviewers:

- Make sure that the question is understood before going to the next question.
- Allow respondents to clarify their responses if possible.
- Write down responses accurately for further analysis.